



Norton
AntiVirusTM 2004
Professional

User's Guide

Norton AntiVirus™ Professional User's Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 10.0

PN: 10098595

Copyright Notice

Copyright © 2003 Symantec Corporation. All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Trademarks

Symantec, the Symantec logo, CleanSweep, Ghost, GoBack, LiveUpdate, Norton AntiVirus, Norton SystemWorks, and Norton Utilities are U.S. registered trademarks of Symantec Corporation. Norton Internet Security, Norton Parental Control, Norton Personal Firewall, Norton Privacy Control, and Norton Productivity Control are trademarks of Symantec Corporation.

Microsoft, MSN, Windows, and the Windows logo are registered trademarks of Microsoft Corporation. AOL and CompuServe are registered trademarks of America Online, Inc. Pentium is a registered trademark of Intel Corporation. Yahoo! is a registered trademark of Yahoo! Inc.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

SYMANTEC SOFTWARE LICENSE AGREEMENT

Norton AntiVirus Professional

IMPORTANT: PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND SYMANTEC. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING THE "ACCEPT" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK THE "I DO NOT ACCEPT" OR "NO" BUTTON OR OTHERWISE INDICATE REFUSAL, MAKE NO FURTHER USE OF THE SOFTWARE AND CONTACT SYMANTEC CUSTOMER SERVICE FOR INFORMATION ON HOW TO OBTAIN A REFUND OF THE MONEY YOU PAID FOR THE SOFTWARE (LESS SHIPPING, HANDLING, AND ANY APPLICABLE TAXES) AT ANY TIME DURING THE SIXTY (60) DAY PERIOD FOLLOWING THE DATE OF PURCHASE.

1. License:

The software and documentation that accompanies this license (collectively the "Software") is the property of Symantec, or its licensors, and is protected by copyright law. While Symantec continues to own the Software, You will have certain rights to use the Software after Your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that Symantec may furnish to You. Except as may be modified by a Symantec license certificate, license coupon, or license key (each a "License Module") that accompanies, precedes, or follows this license, Your rights and obligations with respect to the use of this Software are as follows.

You may:

- A. use one copy of the Software on each of two (2) single computers. If a License Module accompanies, precedes, or follows this license, You may make the number of copies of the Software licensed to You by Symantec as provided in Your License Module. Your License Module shall constitute proof of Your right to make such copies;
- B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of Your computer and retain the original for archival purposes;

C. use the Software on a network, provided that You have a licensed copy of the Software for each computer that can access the Software over that network;

D. after written notice to Symantec, transfer the Software on a permanent basis to another person or entity, provided that You retain no copies of the Software and the transferee agrees to the terms of this license; and

E. use the Software in accordance with any additional permitted uses set forth below.

You may not:

- A. copy the printed documentation that accompanies the Software;
- B. sublicense, rent, or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;
- C. use the Software as part of a facility management, timesharing, service provider, or service bureau arrangement;
- D. use a previous version or copy of the Software after You have received a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;
- E. use a later version of the Software than is provided herewith unless You have purchased upgrade insurance or have otherwise separately acquired the right to use such later version;
- F. use, if You received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which You have not received a permission in a License Module;
- G. use the Software in any manner not authorized by this license; nor
- H. use the Software in any manner that contradicts any additional restrictions set forth below.

2. Content Updates:

Certain Software utilize content that is updated from time to time (including but not limited to the following Software: antivirus software utilize updated virus definitions; content filtering software utilize updated URL lists; some firewall software utilize updated firewall rules; and vulnerability assessment products utilize updated vulnerability data; these updates are collectively referred to as "Content Updates"). You shall have the right to obtain Content Updates for any period for which You have purchased maintenance, except for those Content Updates that Symantec elects to make available by separate paid subscription, or for any period for which You have otherwise separately acquired the right to obtain Content Updates. Symantec reserves the right to designate specified Content Updates as

requiring purchase of a separate subscription at any time and without notice to You; provided, however, that if You purchase maintenance hereunder that includes particular Content Updates on the date of purchase, You will not have to pay an additional fee to continue receiving such Content Updates through the term of such maintenance even if Symantec designates such Content Updates as requiring separate purchase. This License does not otherwise permit the Licensee to obtain and use Content Updates.

3. Product Installation and Required Activation:

There are technological measures in this Software that are designed to prevent unlicensed or illegal use of the Software. You agree that Symantec may use these measures to protect Symantec against software piracy. This Software may contain enforcement technology that limits the ability to install and uninstall the Software on a machine to not more than a finite number of times for a finite number of machines. This License and the Software containing enforcement technology require activation as further set forth during installation and in the Documentation. The Software will only operate for a finite period of time prior to Software activation by You. During activation, You will provide Your unique product key accompanying the Software and PC configuration in the form of an alphanumeric code over the Internet to verify the authenticity of the Software. If You do not complete the activation within the finite period of time set forth in the Documentation, or as prompted by the Software, the Software will cease to function until activation is complete, which will restore Software functionality. In the event You are not able to activate the Software over the Internet, or through any other method specified during the activation process, You may contact Symantec Customer Support using the information provided by Symantec during activation, or as may be set forth in the Documentation.

4. Sixty (60) Day Money Back Guarantee:

If You are the original licensee of this copy of the Software and are not completely satisfied with it for any reason, please contact Symantec Customer Service for a refund of the money You paid for the Software (less shipping, handling, and any applicable taxes) at any time during the sixty (60) day period following the date of purchase.

5. Limited Warranty:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to You. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money You paid for the Software. Symantec does not

warrant that the Software will meet Your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

6. Disclaimer of Damages:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC OR ITS LICENSORS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT, OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S OR ITS LICENSORS' LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether You accept the Software.

7. U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items," as that term is defined in 48 C.F.R. section 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec

Corporation, 20330 Stevens Creek Blvd.,
Cupertino, CA 95014.

8. Export Regulation:

The Software and its related documentation, including technical data, may not be exported or re-exported in violation of the U.S. Export Administration Act, its implementing laws and regulations, the laws and regulations of other U.S. agencies, or the export and import laws of the jurisdiction in which the Software was obtained. Export to any individual, entity, or country specifically designated by applicable law is strictly prohibited.

9. General:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England and Wales.

This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals, and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment, or similar communications between the parties. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. Software and documentation is delivered Ex Works California, U.S.A. or Dublin, Ireland respectively (ICC INCOTERMS 2000).

This Agreement may only be modified by a License Module that accompanies this license or by a written document that has been signed by both You and Symantec. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write to: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A., (ii) Symantec Authorized Service Center, Postbus 1029, 3600 BA Maarssen, The Netherlands, or (iii) Symantec Customer Service, 1 Julius Ave, North Ryde, NSW 2113, Australia.

Contents

Chapter 1	Responding to emergencies	
	If your product won't install	12
	If your computer won't start	13
	Scan for viruses using the CD	13
	Create Emergency Disks	14
	If you need to use Emergency Disks	15
	How to maintain protection	16
	Avoid viruses and threats	16
	Prepare for emergencies	17
 Chapter 2	 Feature summary	
	Activation protects you	20
	When to activate your product	20
	Locate the product key	20
	Virus and threat protection features	21
	Advanced data protection features	23
 Chapter 3	 Installing Norton AntiVirus Professional	
	System requirements	25
	Supported email clients	26
	Unsupported email programs	27
	Supported instant messenger clients	28
	Prepare your computer	28
	Install Norton AntiVirus Professional	28
	After installation	34
	Use the Information Wizard	35
	Read the Readme file	37
	If you need to uninstall Norton AntiVirus Professional	38

Chapter 4**Basics**

Check the version number	39
Start Norton AntiVirus	40
Use the Norton AntiVirus icon in the Windows system tray	40
Use the Windows Explorer toolbar	40
Activate your product	42
Temporarily disable Auto-Protect	43
Check Norton AntiVirus configuration status	45
Check Office Plug-in status	46
Monitor Norton AntiVirus activities	47
About the Log Viewer	47
Check the Activity Log	47
Create and use Rescue Disks	49
About Rescue Disks	49
Create a Rescue Disk set	49
Test your Rescue Disks	51
Update your Rescue Disks	52
Rescue Disk options	52
If you need to use Rescue Disks to restore your system	53
For more information	55
Look up glossary terms	55
Use online Help	55
Readme file	56
Access the User's Guide PDF	56
Symantec products on the Web	57
Subscribe to the Symantec Security Response newsletter	59

Chapter 5**Options**

Customize Norton AntiVirus	62
About System options	62
About Internet options	63
About Other options	64
Set Norton AntiVirus options	65
If you need to restore default Norton AntiVirus settings	66
Password protect Norton AntiVirus options	66

Chapter 6	Keeping current with LiveUpdate	
	About program updates	69
	About protection updates	70
	Obtain updates using LiveUpdate	71
	When you should update	71
	If you can't use LiveUpdate	71
	Set LiveUpdate to Interactive or Express mode	72
	Turn off Express mode	73
	If you run LiveUpdate on an internal network	73
	Run LiveUpdate automatically	74
	About your subscription	76
 Chapter 7	 Protecting disks, files, and data from viruses	
	Ensure that protection settings are enabled	77
	Manually scan disks, folders, and files	79
	Perform a full system scan	79
	Scan individual elements	80
	If problems are found during a scan	81
	Create and use custom scans	81
	Run a custom scan	83
	Delete a custom scan	83
	Schedule scans	83
	Schedule a custom scan	84
	Edit scheduled scans	85
	Delete a scan schedule	86
 Chapter 8	 What to do if a virus is found	
	If a virus is found during a scan	88
	Review the repair details	88
	Use the Repair Wizard	88
	If a virus is found by Auto-Protect	90
	If you are using Windows 98/98SE/Me	90
	If you are using Windows 2000/XP	91
	If a threat is found by Worm Blocking	92
	If Inoculation alerts you about a change in system files	93
	If Norton AntiVirus places files in Quarantine	93
	If Norton AntiVirus cannot repair a file	95
	Look up viruses on the Symantec Web site	96

Chapter 9	Recovering missing or erased files	
	About Norton Protection	97
	About UnErase Wizard	98
	Recover a file with UnErase Wizard	98
Chapter 10	Eliminating data permanently	
	About Wipe Info	101
	About hexadecimal values	102
	About the Government Wipe process	102
	Set Wipe Info options	103
	Wipe files or folders	104
Chapter 11	Troubleshooting	
	Explore the Symantec service and support Web site	107
	Troubleshoot Norton AntiVirus	109
	Auto-Protect does not load when I start my computer	109
	I have scanned and removed a virus, but it keeps infecting my files	110
	Norton AntiVirus cannot repair my infected files	111
	I can't receive email messages	111
	I can't send email messages	112
	Troubleshoot Rescue Disks	113
	My Rescue Disk does not work	113
	I cannot start from drive A	114
	I get an error when testing basic Rescue Disks	115
	Service and support solutions	
	Glossary	
	Index	

Responding to emergencies

1

If you have an emergency, read these sections to try to find the solution to your problem.

Common problems include:

- Virus *threats*
- Trouble restarting your computer
- Lost or missing files
- Possible disk damage



If you purchased this product to address any of the problems listed above, read these sections first. Immediate installation of the product may not always provide the best solution to your problem.

If your product won't install



You must be running Windows in order to install your Symantec product.

If you try to install and your computer has a virus and you choose not to run the Symantec Pre-Install Scanner, start over and run the Symantec Pre-Install Scanner as directed.

If you can't run the Symantec Pre-Install Scanner, but you can connect to the Internet, go to <http://security.symantec.com> and run virus detection from the Symantec Security Check Web site.

If you can't start your computer, you need to start from an uninfected disk and scan for viruses.

Once the virus has been repaired, delete the installation files that were left behind in the temporary folder after you tried to install the first time.


To delete remaining installation files

- 1 On the Windows taskbar, click **Start > Run**.
- 2 In the Run dialog box, type %TEMP%
- 3 Click **OK**.
- 4 In the Temp window, select all of the files.
- 5 Click **Delete**.
- 6 Close the window.
- 7 After you delete the temporary files, begin installation again and run the Symantec Pre-Install Scanner to be sure that you have removed all of the viruses.

See "If your computer won't start" on page 13.

If your computer won't start

If you have a virus or threat on your computer, you need to start the computer from an uninfected disk to remove the virus.

Suggestion	For more information
Restart from the CD and scan your computer's hard disk for viruses.	See "Scan for viruses using the CD" on page 13.
If you have access to another computer, create a set of Emergency Disks and start your computer from the Emergency Disks.	See "Create Emergency Disks" on page 14. See "If you need to use Emergency Disks" on page 15.
Start your computer by using your Rescue Disks if you created them.  Rescue Disks are available only for Windows 98/Me.	See "Create and use Rescue Disks" on page 49.

Scan for viruses using the CD



You might need to change your computer's BIOS Setup options to start from the CD-ROM drive. To do so, see the documentation that came with your computer.

To start from the CD and scan for viruses

- 1 Insert the CD into the CD-ROM drive.
- 2 Restart your computer.
Your computer displays the following information:
 - 1 Boot from Hard Drive
 - 2 Boot from CD-ROM
- 3 Click **2 Boot from CD-ROM** to restart from the CD.
After the computer restarts, the Emergency program automatically begins to scan for and remove viruses.
- 4 When Norton AntiVirus has finished scanning, remove the CD from your CD-ROM drive.

Create Emergency Disks

Emergency Disks are used to start your computer in case of a problem. If your computer can start from a CD, you can use the product CD in place of Emergency Disks and do not need to create them.

If you downloaded the software or do not have a CD, the program for creating Emergency Disks (NED.exe) is included in the download. Navigate to the location to which you downloaded the software and begin with step 3 of these instructions.

See "If you need to use Emergency Disks" on page 15.

If you cannot start your computer from a CD, you can use these instructions to create Emergency Disks on another computer or go to <http://www.symantec.com/techsupp/ebd.html> and download the Emergency Disk program. Follow the instructions included in the download to create the Emergency Disks.



You will need several formatted 1.44-MB disks.

To create Emergency Disks from the CD

- 1 Insert the CD into the CD-ROM drive.
- 2 Click **Browse CD**.
- 3 Double-click the **Support** folder.
- 4 Double-click the **Edisk** folder.
- 5 Double-click **NED.exe**.
- 6 In the welcome window, click **OK**.
- 7 Label the first disk as instructed and insert it into drive A.
- 8 Click **Yes**.
- 9 Repeat steps 7 and 8 for the subsequent disks.
- 10 When the procedure is complete, click **OK**.
- 11 Remove the final disk from drive A and store the Emergency Disk set in a safe place.

If you need to use Emergency Disks

See ["Create Emergency Disks"](#) on page 14.

If you have not created Rescue Disks, you can use Emergency Disks to restart your computer and scan for viruses.

To use Emergency Disks

- 1 Insert Emergency Disk 1 into drive A and restart your computer.
The Emergency program runs in DOS.
- 2 Ensure that Antivirus is selected, then press **Enter**.
- 3 Follow the on-screen instructions for inserting and removing the Emergency Disks.
The Emergency program automatically scans your computer and removes viruses.
- 4 When the Emergency program is done, remove the Emergency Disk from drive A and restart your computer.

How to maintain protection

When Norton AntiVirus is installed, you have complete virus protection. However, new viruses and threats are created constantly. Viruses can spread when you start your computer from an infected disk or when you run an infected program. There are several things that you can do to avoid viruses and to recover quickly should a virus strike.

Avoid viruses and threats

It is important that you practice regular file maintenance and that you keep Norton AntiVirus up-to-date.

To avoid viruses:

- Write-protect removable media.
- Stay informed about viruses by logging on to the Symantec Security Response Web site (<http://securityresponse.symantec.com>) where there is extensive, frequently updated information on viruses and automatic virus protection.
- Keep LiveUpdate turned on at all times to continually update your virus definitions files.
- Run LiveUpdate regularly to receive new program updates.
- Keep Auto-Protect turned on at all times to prevent viruses from infecting your computer.
- If Auto-Protect is not turned on, scan removable media before you use them.
- Schedule periodic scans to occur automatically.
- Watch for email messages from unknown senders. Do not open anonymous attachments.
- Keep email protection turned on to avoid sending or receiving infected email attachments.
- Keep all recommended maximum protection settings turned on.

See "Explore the Symantec service and support Web site" on page 107.

See "Keeping current with LiveUpdate" on page 69.

See "Manually scan disks, folders, and files" on page 79.

See "Schedule scans" on page 83.

See "Ensure that protection settings are enabled" on page 77.

Prepare for emergencies

It is also important that you are prepared in case your computer is infected by a virus.

To prepare for emergencies:

- Back up files regularly and keep more than just the most recent backup.
- If you are using a computer that cannot start from a CD, create a set of Emergency Disks, from which you can start your computer and scan for viruses.
- If you are using Windows 98/Me, create a set of Rescue Disks and keep them updated. You can use them to start your computer in DOS mode and use Norton AntiVirus to fix virus-related problems and recover from a system crash.

See ["Create Emergency Disks"](#) on page 14.

See ["Create and use Rescue Disks"](#) on page 49.



Feature summary

2

Use the information in this section to familiarize yourself with the product.

This section includes:

- A list of all of the features in the product
- A brief description of each feature

The feature summary can help you determine which feature to use to solve a problem. Read the feature descriptions to locate the correct component to use.

Activation protects you

Product activation is a technology that protects users from pirated or counterfeit software by limiting use of a product to those users who have acquired the product legitimately. Product activation requires a unique product key for each installation of a product. You must activate the product within 15 days of installing it.

Product activation is completely separate from registration. Your activation information and registration information reside on separate servers, with no link between the different sets of data.

When to activate your product

During installation, you are asked to enter a product key. After you have installed the product, activate it by sending the product key to the Symantec servers.

You can activate your product by clicking **Activate Now** in the Activation Wizard that runs immediately after installation. If you choose not to activate at that time, you will receive [alerts](#) that will remind you to activate the product. You can click **Activate Now** in the alerts to activate the product. Activation should take just a few minutes.



If you do not activate the product within 15 days of installing it, the product will stop working. You can activate it after the 15 days have elapsed, but you will not be protected until you do.

Locate the product key

The product key can most frequently be found on a sticker on your CD sleeve. If it is not there, then it will be on an insert in your product package. If you have purchased the product on DVD, look for the sticker on your DVD package. If you have [downloaded](#) the product from the Symantec Store, the product key is stored on your computer as part of the download process.

Virus and threat protection features

Norton AntiVirus provides comprehensive virus prevention, threat detection, and repair software for your computer. It automatically detects and repairs known viruses. Norton AntiVirus detects viruses and other potential risks in instant messenger attachments as well as in email messages, Internet downloads, and other files. Easy updating of the [virus definitions](#) over the Internet keeps Norton AntiVirus prepared for the latest [threats](#).

Norton AntiVirus now includes expanded threat detection of both known and emerging threats, such as spyware and other files that could put your computer at risk. Norton AntiVirus also scans files inside of compressed files.

As always, Norton AntiVirus features continually monitor your computer and protect it from known and unknown threats.

Feature	Description
Auto-Protect	<ul style="list-style-type: none"> ■ Loads into memory when Windows starts, providing constant protection while you work. ■ Checks for viruses every time that you use software programs on your computer, insert floppy disks or other removable media, access the Internet, or use document files that you receive or create. ■ Monitors your computer for any unusual symptoms that may indicate an active threat. <p>See "What to do if a virus is found" on page 87.</p>
Virus protection updates	<p>Updates your virus definitions automatically.</p> <p>See "About protection updates" on page 70.</p>
Compressed file protection	<p>Detects and repairs viruses inside of compressed files.</p> <p>See "What to do if a virus is found" on page 87.</p>

Feature	Description
Email protection	Protects incoming and outgoing email messages, preventing your computer and other computers from infection. See "What to do if a virus is found" on page 87.
Instant messenger protection	Scans for and detects viruses in instant messenger attachments. See "What to do if a virus is found" on page 87.
Bloodhound technology	Detects new and unknown viruses by analyzing an executable file's structure, behavior, and other attributes such as programming logic, computer instructions, and any data that is contained in the file. See "What to do if a virus is found" on page 87.
Password protection	Protects Norton AntiVirus options from unauthorized changes. See "Password protect Norton AntiVirus options" on page 66.

Advanced data protection features

UnErase Wizard and Wipe Info tools help you recover lost data and permanently wipe or erase the contents of a file to protect sensitive information.

Feature	Description
UnErase Wizard	Locates and recovers files that are protected by Norton Protection or the Windows Recycle Bin. See " About UnErase Wizard " on page 98.
Wipe Info	Permanently removes unwanted files so that they can never be recovered by a file recovery program. Wipe Info can also wipe the free space on your hard disk, ensuring that previously deleted information does not remain on your hard disk. See " About Wipe Info " on page 101.



Installing Norton AntiVirus Professional

3

Before installing Norton AntiVirus Professional, take a moment to review the system requirements that are listed in this chapter. Windows 98/Me users should have several blank 1.44-MB disks available to make Rescue Disks.

System requirements

To use Norton AntiVirus Professional, your computer must have one of the following Windows operating systems:

- Windows 98/98SE/Me
- Windows 2000 Professional
- Windows XP Professional/Home Edition

Installation of Norton AntiVirus Professional is not supported on Windows 95/NT 4.0, Macintosh, Linux, or server versions of Windows 2000/XP computers.



If you are planning to upgrade your Windows operating system from Windows 98/Me to Windows 2000/XP, you must uninstall Norton AntiVirus Professional first and then reinstall after the upgrade is complete.

Your computer must also meet the following minimum requirements.

Operating system	Requirements
Windows 98/98SE/Me	<ul style="list-style-type: none"> ■ 133-MHz processor for Windows 98; 150-MHz processor for Windows Me ■ 32 MB of RAM ■ 125 MB of available hard disk space ■ CD-ROM or DVD-ROM drive ■ Internet Explorer 5.1 with Service Pack 2 or later (5.5 recommended)
Windows 2000 Professional Edition	<ul style="list-style-type: none"> ■ 133-MHz or higher processor ■ 64 MB of RAM ■ 85 MB of available hard disk space ■ CD-ROM or DVD-ROM drive ■ Internet Explorer 5.1 with Service Pack 2 or later (5.5 recommended)
Windows XP Professional/Home Edition Service Pack 1 Windows XP Tablet PC and Media Center Editions	<ul style="list-style-type: none"> ■ 300-MHz or higher processor ■ 128 MB of RAM ■ 85 MB of available hard disk space ■ CD-ROM or DVD-ROM drive ■ Internet Explorer 5.1 with Service Pack 2 or later (5.5 recommended)



If you are installing on Windows 2000/XP, you must install with administrator privileges.

Supported email clients

Email scanning is supported for any *POP3*-compatible and SMTP-compatible email client including:

- Microsoft Outlook Express version 4, 5, or 6
- Microsoft Outlook 97/98/2000/XP
- Netscape Messenger version 4, Netscape Mail version 6

- Eudora Light version 3, Eudora Pro version 4, Eudora version 5
- Pegasus 4

Unsupported email programs

Norton AntiVirus does not support the following email clients:

- IMAP
- AOL
- POP3s with Secure Sockets Layer (SSL)
See the online Help for more information about Secure Sockets Layer connections.
- Web-based email such as Hotmail and Yahoo!
- Lotus Notes

About encrypted email connections

Norton AntiVirus does not support email connections using Secure Sockets Layer (SSL). SSL is a Netscape protocol designed to provide secure communications on the Internet. If you use an SSL connection, you are not protected by Norton AntiVirus.

To send email messages through SSL connections, disable incoming and outgoing email protection in Norton AntiVirus.

To send email through an SSL connection

- 1 In the main window, click **Options**.
If a menu appears, click **Norton AntiVirus**.



If you set a password for Options, Norton AntiVirus Professional asks you for the password before you can continue.

- 2 In the Options window, click **Email**.
- 3 Click **OK**.
- 4 Uncheck **Scan incoming Email (recommended)**.
- 5 Uncheck **Scan outgoing Email (recommended)**.
- 6 Resend your email.

Supported instant messenger clients

The following instant messenger clients are supported:

- AOL Instant Messenger, version 4.7 or later
- Yahoo! Messenger, version 5.0 or later
- MSN Messenger, versions 4.6 and 4.7
- Windows Messenger, version 4.6 or later for Windows XP

Prepare your computer

See ["Create Emergency Disks"](#) on page 14.

See ["If you need to uninstall Norton AntiVirus Professional"](#) on page 38.

Before you install Norton AntiVirus, prepare your computer. If your computer cannot start from a CD, create Emergency Disks.

If you have an earlier version of Norton AntiVirus Professional, the new version automatically removes the earlier version. If your version is earlier than 2002, you must uninstall it before installing the new version. If you have Norton AntiVirus Professional 2002, you can transfer your existing option settings to the new version of the program.

Before you install Norton AntiVirus, use these suggestions to prepare your computer:

- If you have any other antivirus programs on your computer, you must uninstall them and restart your computer before installing Norton AntiVirus Professional.
To uninstall other antivirus programs, see the user documentation that came with each program.
- Close all other Windows programs before installing Norton AntiVirus Professional, including those programs displayed in the Windows system tray.

Install Norton AntiVirus Professional

Install Norton AntiVirus from the CD or if you downloaded your copy of the product, follow the instructions on the Web page.

If you have not already done so, close all other Windows programs.

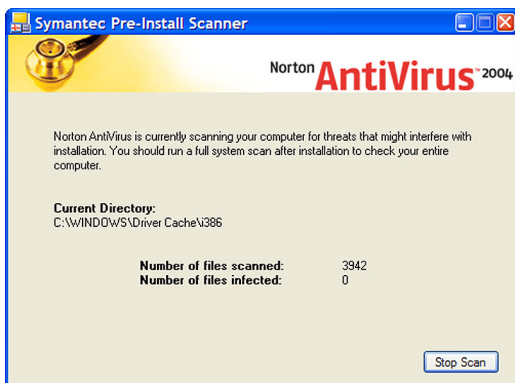
To install Norton AntiVirus Professional from the CD

- 1 Insert the CD into the CD-ROM drive.



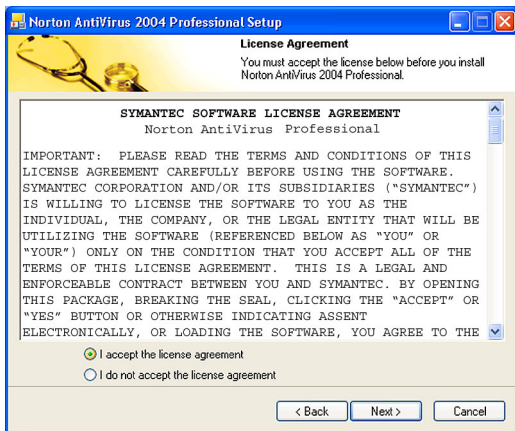
If your computer is not set to automatically open a CD, you will have to open it yourself.

- 2 In the Norton AntiVirus Professional window, click **Install Norton AntiVirus Professional**.
- 3 In the Scan for Viruses dialog box, click **Yes** to scan your computer before installing Norton AntiVirus.



- 4 In the Symantec Pre-Install Scanner window, review the progress of the scan.
 If Norton AntiVirus detects a virus, it prompts you to delete each file individually.
- 5 Click **Delete** for each file that you want to delete.
- 6 After the scan completes, view the results in the scanresults -Notepad window, then exit Notepad.

- 7 In the Norton AntiVirus 2004 Professional Setup window, click **Next** to continue with the installation.



- 8 Read the License Agreement, then click **I accept the license agreement**.
If you decline, you cannot continue with the installation.

9 Click **Next**.

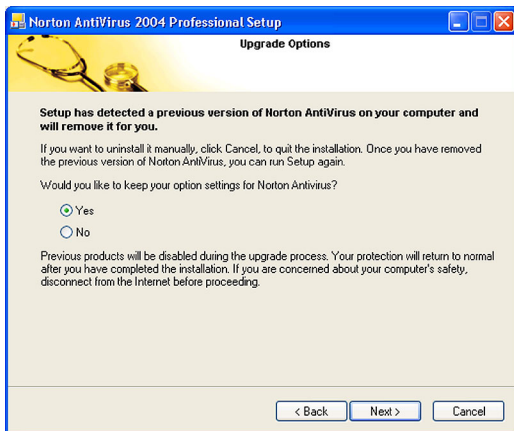


See ["Activation protects you"](#) on page 20.

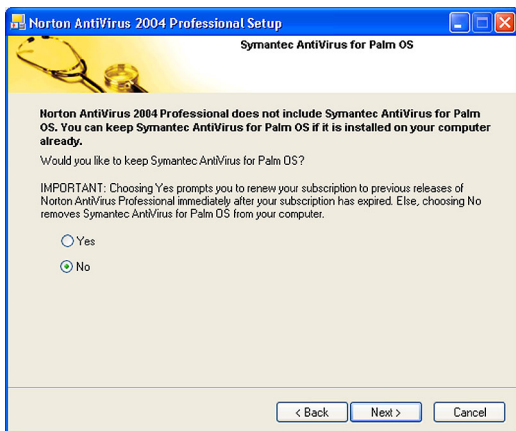
10 In the Activation window, type the product key for activation, then click **Next**.



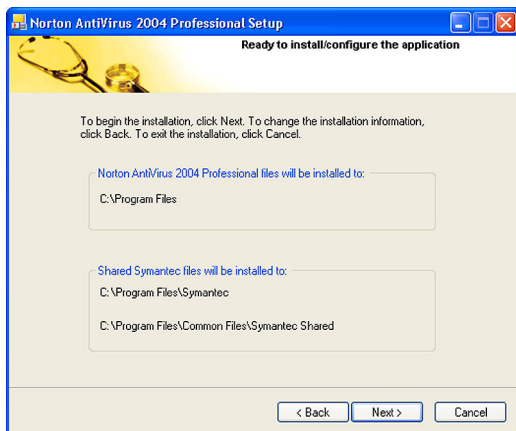
- 11 Select a folder into which you want to install Norton AntiVirus Professional, then click **Next**.



- 12 If you are upgrading from Norton AntiVirus 2002 or 2003, you can keep your option settings. Click **Yes** to keep your option settings, then click **Next**.



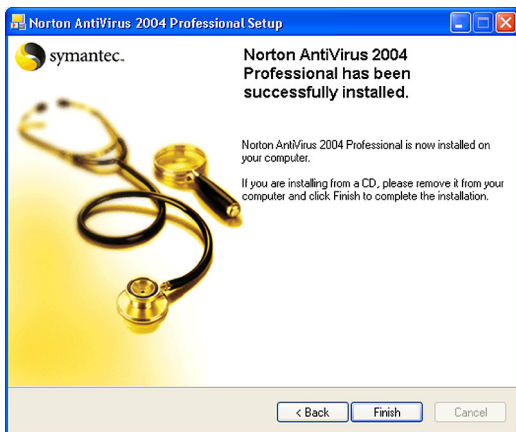
- 13** If you have Norton AntiVirus 2001 or 2002 Professional Edition installed on your computer, you can keep the Symantec AntiVirus for Palm OS component installed. Click **Yes** to keep the component installed, then click **Next**.



- 14** Confirm the installation location, then click **Next**.

See ["Read the Readme file"](#) on page 37.

- 15 After Norton AntiVirus Professional is installed, scroll through the Readme text, then click **Next**.



- 16 Click **Finish** to complete the installation.



After installation, you must restart your computer for all Norton AntiVirus options to be enabled.

After installation

For Windows 98/Me, you must restart your computer after installing Norton AntiVirus Professional.

If your computer needs to be restarted after Norton AntiVirus Professional is installed, a prompt appears giving you the option to do so immediately. After restarting or if your computer does not need to be restarted, the Information Wizard appears.



If you bought your computer with Norton AntiVirus already installed, the Information Wizard appears the first time that you start Norton AntiVirus Professional. You must accept the license agreement that appears in the Information Wizard to activate Norton AntiVirus.

Use the Information Wizard

The Information Wizard lets you activate your copy of Norton AntiVirus Professional, get information about your Norton AntiVirus Professional subscription, select post-installation tasks to be done automatically, and review your Norton AntiVirus Professional settings.



If you choose not to register the software using the Information Wizard or if registration fails for some reason, you can register by using the Product Registration option on the Help menu or by using the Symantec Web site at www.symantec.com. On the Web site, go to the Products page for the registration link.

To use the Information Wizard

- 1 In the welcome window, click **Next**.



You must activate the software within 15 days.

See “[Activation protects you](#)” on page 20.

- 2 On the Product Activation window, click **Activate and register your product now**.
- 3 Click **Next**.
- 4 Make sure that your computer is connected to the Internet, then click **Next**.
- 5 If you purchased your computer with Norton AntiVirus already installed, you must accept the license agreement in order to use Norton AntiVirus Professional. Click **I accept the license agreement**, then click **Next**.
- 6 In the first Registration window, select the Country/Region from which you are registering.
- 7 If you would like information from Symantec about Norton AntiVirus Professional, check the method by which you want to receive that information, type the corresponding address and phone number, then click **Next**.
- 8 Check if you would like to receive postal mail from Symantec.
- 9 Type your name and address, then click **Next**.

See “[Activate your product](#)” on page 42.

- 10
- Make sure your computer is connected to the Internet, then click **Next** to activate.
- 11
- Click **Finish**.
- 12
- Select the post-installation tasks that you want Norton AntiVirus Professional to perform automatically. Your options are:

Run LiveUpdate	Ensure that you have the latest virus definitions. See "Keeping current with LiveUpdate" on page 69.
Create a Rescue Disk Set	If you are installing in Windows 98/Me, you also have the option to create a Rescue Disk set. See "Create and use Rescue Disks" on page 49.
Scan for Viruses	Perform a full system scan. See "Manually scan disks, folders, and files" on page 79.
Schedule weekly scans of local hard drives	Schedule a weekly scan of your local hard drives. You must have Microsoft Scheduler installed to use this option. If you select this option, you can change the schedule for this scan as desired. See "Schedule scans" on page 83.
Enable Auto-Protect to scan inside of compressed files	Set the option to scan compressed files automatically by Auto-Protect. See "About System options" on page 62.

See ["Customize Norton AntiVirus"](#) on page 62.

- 13
- Click **Next**.
- 14
- Review the post-installation tasks and configuration settings for Norton AntiVirus Professional.
If you want to change any of the settings, do so using Options.
- 15
- Click **Finish**.

If you selected any post-installation tasks, they start automatically.

Read the Readme file

The Readme file contains technical tips and information about product changes that occurred after this guide went to press. It is installed on your hard disk in the same location as the Norton AntiVirus Professional product files.

To read the Readme file

- 1 Using Windows Explorer, navigate to the location in which your Norton AntiVirus Professional files are installed.
If you installed Norton AntiVirus Professional in the default location, the files are in C:\Program Files\Norton AntiVirus Professional.
- 2 Double-click **Readme.txt** to open the file in Notepad or Wordpad.
The Readme file includes instructions for printing it if you want to do so.
- 3 Close the word-processing program when you are done reading the file.

If you need to uninstall Norton AntiVirus Professional

If you need to remove Norton AntiVirus Professional from your computer, you can use the Add/Remove Programs option in the Windows Control Panel.



During uninstallation, Windows may indicate that it is installing software. This is a standard Microsoft installation message and can be disregarded.

To uninstall Norton AntiVirus Professional from the Windows Control Panel

- 1 Do one of the following:
 - On the Windows taskbar, click **Start > Settings > Control Panel**.
 - On the Windows XP taskbar, click **Start > Control Panel**.
- 2 In the Control Panel, double-click **Add/Remove Programs**.
- 3 In the list of currently installed programs, click **Norton AntiVirus Professional**.
- 4 Do one of the following:
 - In Windows 98/Me, click **Add/Remove**.
 - In Windows 2000/XP, click **Remove**.
- 5 Click **Remove All** to confirm that you want to uninstall the product.
- 6 If you have files in Quarantine, you are asked if you want to delete them. Your options are:

Yes	Deletes the quarantined files from your computer
No	Leaves the quarantined files on your computer, but makes them inaccessible

- 7 Click **Reboot Now**, then click **Finish**.

Basics include general information about how to:

- Work with your Symantec product.
- Keep your computer protected.
- Customize options.
- Monitor protection activities.
- Access more information.

Check the version number

You can check the version number of your product on your computer. Use the version number to help you find more information about your product on the Symantec Web site.

To check the version number

- 1 Start your product.
- 2 Click **Help and Support**.
- 3 On the Help menu, click **About <your product name>**.
- 4 In the About dialog box, select your product name.

Start Norton AntiVirus

After installation, Norton AntiVirus automatically protects any computer on which it is installed. You do not have to start the program to be protected.

To start Norton AntiVirus

- ❖ Do one of the following:
 - On the Windows taskbar, click **Start > Programs > Norton AntiVirus > Norton AntiVirus 2004**.
 - On the Windows XP taskbar, click **Start > More Programs > Norton AntiVirus > Norton AntiVirus 2004**.
 - On the desktop, double-click the Norton AntiVirus Professional icon.

Use the Norton AntiVirus icon in the Windows system tray

See ["Customize Norton AntiVirus"](#) on page 62.

Norton AntiVirus adds an icon to the Windows system tray at the end of the Windows taskbar. Use the icon in the Windows system tray to open Norton AntiVirus and to enable or disable Auto-Protect.

To use the Norton AntiVirus Windows system tray icon

- ❖ In the Windows system tray, right-click the Norton AntiVirus icon, then on the tray icon menu, select the option that you want.

Use the Windows Explorer toolbar

Norton AntiVirus adds a button and menu to Windows Explorer.

When you first open Windows Explorer after installing Norton AntiVirus, you may not see the Norton AntiVirus button and menu. You might have to restart Windows before the toolbar button appears.



You may not be able to access the Norton AntiVirus Windows Explorer menu, depending on your computer's configuration.

To display the Norton AntiVirus button and menu

- 1 On the View menu, click **Toolbars > Norton AntiVirus**.
- 2 Click the arrow to the right of the button to view your options. Your options are:

View Status	<p>Launches Norton AntiVirus and displays the Status window with system status.</p> <p>See "Check Norton AntiVirus configuration status" on page 45.</p>
View Quarantine	<p>Displays the Quarantine area and the files currently stored there.</p> <p>See "If Norton AntiVirus places files in Quarantine" on page 93.</p>
View Activity Log	<p>Displays the Log Viewer, which shows you various Norton AntiVirus activities, such as scans performed and problems found.</p> <p>See "Monitor Norton AntiVirus activities" on page 47.</p>
View Virus Encyclopedia	<p>Connects you to the Symantec Security Response Web page, from which you can search for information on all types of viruses.</p>
Launch Scan Menu	<p>Opens Norton AntiVirus in the Scan for Viruses pane, on which you can specify a scan to run.</p>

Activate your product



Product activation reduces software piracy and ensures that you have received genuine Symantec software.

You must activate your product within 15 days of installing it or the product will stop working.

If you did not activate your product using the Information Wizard, you will receive an Activation Needed *alert* every day until you activate the product.

You can activate your product from the Activation Needed alert or from the Activation option on the Help menu. Activation should take just a few minutes.

To activate your product from the Activation Needed alert

- 1 In the alert, click **Activate Now**.
- 2 Click **OK**.
- 3 On the Activation screen, click **Next**.
- 4 On the Activation Successful screen, click **Finish**.

To activate your product from the Help menu

- 1 At the top of the main window, click **Help and Support > Activation**.
- 2 On the Activation screen, click **Next**.
- 3 On the Activation Successful screen, click **Finish**.

Temporarily disable Auto-Protect

If you have not changed the default option settings, Auto-Protect loads when you start your computer to guard against viruses, Trojan horses, worms, and other malicious threats. It checks programs for viruses as they are run and monitors your computer and removable media for any activity that might indicate the presence of a virus. When a virus or virus-like activity is detected, Auto-Protect alerts you.

In some cases, Auto-Protect may warn you about a virus-like activity that you know is not the work of a virus. If you will be performing such an activity and want to avoid the warning, you can temporarily disable Auto-Protect.



If you have set a password for Options, Norton AntiVirus Professional asks you for the password before you can view or adjust the settings.

See "Start Norton AntiVirus" on page 40.

To temporarily disable Auto-Protect

- 1 In the main window, click **Options**.
If a menu appears, click **Norton AntiVirus**.
- 2 In the Options window, under System, click **Auto-Protect**.
- 3 In the Auto-Protect pane, uncheck **Enable Auto-Protect**.

Be sure to enable Auto-Protect when you have completed your task to ensure that your computer remains protected.

To enable Auto-Protect

- 1 In the main window, click **Options**.
If a menu appears, click **Norton AntiVirus**.
- 2 In the Options window, under System, click **Auto-Protect**.
- 3 In the Auto-Protect pane, check **Enable Auto-Protect**.

If the Norton AntiVirus Professional icon appears in the Windows system tray, you can use it to enable and disable Auto-Protect.

Temporarily disable Auto-Protect

To enable or disable Auto-Protect using the icon in the Windows system tray

- ❖ In the Windows system tray, right-click the Norton AntiVirus Professional icon, then do one of the following:
 - If Auto-Protect is disabled, click **Enable Auto-Protect**.
 - If Auto-Protect is enabled, click **Disable Auto-Protect**.

Check Norton AntiVirus configuration status

If Norton AntiVirus is behaving in an unexpected way, or if you're not sure that everything is being scanned for viruses, check the status on the main window.

In the System Status pane of the Norton AntiVirus main window, a check mark indicates that the system status is OK and a triangle indicates that your system needs attention. If you see a triangle, review the features to see which area needs attention.

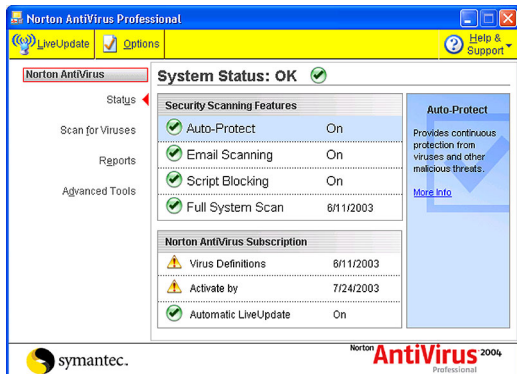
If you see an exclamation point, it indicates that your subscription is either expired or your virus definitions are more than two weeks old. If your subscription is expired, renew it to maintain your protection. If your subscription is current, then you need to update your virus definitions.

If you need to adjust any settings, use Options.

See ["Customize Norton AntiVirus"](#) on page 62.

To check system status

- 1 In the main window, under Norton AntiVirus, click **Status**.



Check Norton AntiVirus configuration status

- 2 In the System Status pane, review the status to the right of each feature.
- 3 For information about a particular feature, select the feature.
The right pane displays a description and a link to more information about the feature.

Check Office Plug-in status

Office Plug-in protects Microsoft Office documents from viruses, worms, and virus-like activities. It scans documents whenever you open them in a Microsoft Office program. Office Plug-in is enabled in Options.



If you have set a password for Options, Norton AntiVirus asks you for the password before you can view or adjust the settings.

To check Office Plug-in status

- 1 In the main window, click **Options**.
If a menu appears, click **Norton AntiVirus**.
- 2 In the left pane of the Options window, under Other, click **Miscellaneous**.
- 3 Verify that Office Plug-in is enabled.

Monitor Norton AntiVirus activities

Occasionally, you may need to look at previous Norton AntiVirus activities, such as when the last system scan was done or how many viruses were detected last week. Norton AntiVirus displays a record of its threat detection, application, and error activities in the Log Viewer.

About the Log Viewer

The Log Viewer displays the history of activities in each Activity Log. An Activity Log is a collection of multiple log files, one for each type of information collected: threat alerts, application activities, and errors.

Using the information in the Log Viewer, you can:

- View detailed information recorded in each log by selecting the log in the left column and viewing the details in the right pane.
- Delete the activity entries for a log by selecting the log, then clicking Clear. If you never clear the entries for a category, it expands until it reaches the maximum size. Then it starts overwriting the oldest entries.

Check the Activity Log

Check the Activity Log to see what tasks were performed and the results of those tasks to make sure that your Options settings are appropriate for your particular needs.

To check the Activity Log

- 1 In the main window, under Norton AntiVirus, click **Reports**.
- 2 In the Reports pane, on the Activity Log line, click **View Report**.
- 3 In the left pane, select the log that you want to review. Your options are:

Threat alerts	A history of threat alerts, such as the ID and type of threat, date and time when it occurred, the action taken, and the version of the virus definitions used.
Application activities	A history of scanning activities, such as when scanning occurred and with what results.
Errors	Detailed information about any problems encountered when scanning your computer such as the date, error code, and message.

As you select each log, the right pane changes and displays details specific to the particular log. The most recent activities appear at the top of the log.

- 4 When you are finished viewing the information, click **File > Exit**.

Create and use Rescue Disks



Rescue Disks are available only for Windows 98/Me.

Rescue Disks are images on floppy disks that let you restart your computer when your hard disk is damaged or infected with a virus.

About Rescue Disks

Rescue Disks record a duplicate set of system startup files and disk partition information, and store rescue utilities, configuration files, and a DOS-based Norton AntiVirus scanner across multiple floppy disks or on a network drive.

A Rescue Disk set consists of one *bootable* floppy disk, one Norton AntiVirus Program floppy disk, and three Virus Definition floppy disks. If you have Norton Utilities installed, you will also have two Norton Utilities floppy disks in your Rescue Disk set. With a Rescue Disk set, you can start your computer in DOS mode and use Norton AntiVirus to fix virus-related problems.



Rescue Disks contain information specific to the computer on which they were made.

If you are using Rescue Disks for recovery, you must use the disks made for your computer.

If you are using Rescue Disks to scan for viruses, you can use disks made for a different computer.

You should update Rescue Disks whenever you update your virus protection, install new software, or make changes to your hardware.

See ["If you need to use Rescue Disks to restore your system"](#) on page 53.

Create a Rescue Disk set

You can create Rescue Disks any time. You can start the Rescue Disk Wizard from the main window of your Symantec product.

See ["Temporarily disable Auto-Protect"](#) on page 43.

If you start the Rescue Disk Wizard from the main window, temporarily disable Auto-Protect while you are creating the Rescue Disk set. If you do not restart your computer after creating Rescue Disks, remember to enable Auto-Protect again.

When you select a floppy disk drive, the Rescue Disk program calculates the number of disks that you will need to complete the set. Depending on what items you want to include in the Rescue Disk set, you might need ten or more floppy disks.



If you choose to create Rescue Disks on a network drive, a second physical hard disk, or some other large capacity disk drive (but not a CD), your Rescue Disk set is placed in a folder on the selected disk. Make sure that you also have a bootable floppy disk in a safe location. This disk should contain the network [drivers](#) or other files necessary to start your computer and access the drive on which you placed your Rescue Disk set. Creating a Rescue Disk set on a startup hard disk, for example, drive C, is not recommended because you will not be able to access the rescue programs and configuration files if your hard disk is damaged and unable to start.

To create Rescue Disks

- 1 In the main window, click **Rescue**.
- 2 In the Rescue Disk window, select the drive on which to create the Rescue Disk set.
To create a Rescue Disk set on floppy disks, select drive A.
When you select a floppy disk drive, the Basic Rescue program displays the number of floppy disks that you will need to create the Rescue Disk set.
- 3 To make changes to the default Rescue Disk settings, click **Options** and do the following:
 - On the Rescue Files tab, specify the files to include in the Rescue Disk set. If you change the default file selection, the number of required floppy disks will also change.
 - On the Format Settings tab, select the type of format, if any, that you want Rescue Disk to use

when it prepares the bootable floppy disk for the Rescue Disk set.

- 4 Click **OK** to return to the Rescue Disk window.
- 5 When you have either assembled the required number of floppy disks or identified another location for the Rescue Disk files, click **Create**.
 If you selected a floppy disk drive, Rescue Disk displays the Basic Rescue Disk List window and an estimate of how much time you will need to create the entire set.
- 6 Label the disks as specified in the Basic Rescue Disk List window, then click **OK**.
 Rescue Disk prompts you to insert the first disk in the floppy disk drive. If you selected a network drive or other larger-format drive, Rescue Disk prompts you for a Rescue Folder drive location.
- 7 Insert the disks as requested.
- 8 When you have finished creating the basic Rescue Disk set, in the Rescue Disk window, click **Close**.

Test your Rescue Disks

After you have created the Rescue Disk set, you are prompted to test your disks. This requires that you restart your computer using the Rescue Disks.



If you created Rescue Disks on a network drive, a second physical hard disk, or some other large capacity disk drive, you will have to restart into DOS from an external floppy disk, navigate to the Rescue folder, and run Rescue.exe.

To test your Rescue Disks

- 1 Close all open Windows programs.
- 2 Insert the disk labeled Basic Rescue Boot Floppy Disk into drive A, then click **Restart**.
 If the Rescue Disk screen appears on your monitor, the Rescue Disk works properly.
 If the Rescue Disk screen does not appear, you have several options for correcting the problem.
- 3 Press **Escape** to exit to DOS.

See “My Rescue Disk does not work” on page 113.

- 4

Remove the disk from drive A and slide open the plastic tab on the back of the disk to write-protect it.
- 5

Restart your computer.

Update your Rescue Disks

You can update your Rescue Disks as often as you like. Rescue Disk lets you update your basic Rescue Disk set without having to recreate them.

If you are updating a floppy disk set, make sure that your disks are not write-protected before you begin.

To update your Rescue Disks

- 1

In the main window, click **Rescue**.
- 2

In the Rescue Disk window, under Select Destination Drive, click **drive A**, then click **Update**.
A message prompts you to insert the disk labeled Basic Rescue Boot Floppy Disk into drive A.
- 3

Insert the Basic Rescue Boot Floppy Disk into drive A, then click **OK**.
- 4


Insert the remaining disks in your set as requested.

Make sure to test your newly updated Rescue Disk set when prompted.

See ["Test your Rescue Disks"](#) on page 51.

Rescue Disk options

Rescue Disk has the following options.

Add Files	Click to specify additional files that you want Rescue Disk to store on the Rescue Disk set.  Do not use this as a backup utility. Add files only if they are needed to restore your system after a crash.
Remove File	Click to remove the selected file under User-selected Files. The files will no longer be included on the Rescue Disk set.

If you need to use Rescue Disks to restore your system

Rescue items list	<p>The list is categorized and presented in a hierarchical view, similar to a Windows Explorer view. Click the plus sign next to a category to expand the list and see what the category contains. Click the plus sign next to a specific file for more information about the file.</p> <p>The list of rescue items is different depending on the programs you have installed and the type of Rescue Disk set you are using.</p>
Basic Rescue Boot Floppy Files	Files that Rescue Disk stores on the floppy disk that you use to start your system.
Rescue DOS Utility Programs	DOS-based emergency programs that Rescue Disk stores on the Rescue Disk set. You can use these DOS-based utilities to recover your system.
Norton AntiVirus Program	Norton AntiVirus program files.
Definitions Disks	Virus definitions files used by Norton AntiVirus to scan your system in an emergency. There are several of these disks.
User-selected Files	Files you have added to the Rescue Disk set. Add files to this list by clicking Add Files. Remove files from this list by clicking the file, then clicking Remove File.

If you need to use Rescue Disks to restore your system



Rescue Disks are available only for Windows 98/Me.

Sometimes a virus or threat prevents your computer from starting normally. Some viruses can only be removed if the computer is started from a clean disk, not the infected hard disk. Often, a Norton AntiVirus *alert* tells you when to use your Rescue Disks.

If you need to use Rescue Disks to restore your system

You first need to determine if your Rescue Disks are current. This means that you have created or updated your Rescue Disks since you did any of the following:

- Added, modified, or removed internal hardware
- Added, modified, or removed hard disk partitions
- Upgraded your operating system
- Updated virus definitions

If your Rescue Disks are not current, you can still use them to remove viruses from your computer. When the Rescue Disk screen appears, use only the Norton AntiVirus task.

To use your Rescue Disks

- 1 Insert the Basic Rescue Boot Floppy Disk into drive A and restart your computer.
The Rescue program runs in DOS.
- 2 Use the arrow keys to select the program that you want to run.
A description of the selected program appears in the right pane of the Rescue program. Your options are:

Norton AntiVirus	Scans your computer for viruses and repairs any infected files
Rescue Recovery	Checks and restores boot and partition information

- 3 Press **Enter** to run the selected program.
- 4 Follow the on-screen instructions for inserting and removing the Rescue Disks.
- 5 When the Rescue program is done, remove the Rescue Disk from drive A and restart your computer.

For more information

The product documentation provides glossary terms, online Help, a Readme file, the User's Guide in PDF format, and links to the Knowledge Base on the Symantec Web site.

Look up glossary terms

Technical terms that are italicized in the User's Guide are defined in the glossary, which is available in both the User's Guide PDF and Help. In both locations, clicking a glossary term takes you to its definition.

Use online Help

Help is available throughout your Symantec product. Help buttons or links to more information provide information that is specific to the task that you are completing. The Help menu provides a comprehensive guide to all of the product features and tasks that you can complete.

To use online Help

- 1 At the top of the main window, click **Help & Support > Norton AntiVirus Professional**.
- 2 In the Help window, in the left pane, select a tab. Your options are:

Contents	Displays the Help by topic
Index	Lists Help topics in alphabetical order by key word
Search	Opens a search field in which you can enter a word or phrase

Window and dialog box Help

Window and dialog box Help provides information about the program. This type of Help is context-sensitive,

meaning that it provides help for the dialog box or window that you are currently using.

To access window or dialog box Help

- ❖ Do one of the following:
 - In the window, click any available Help link.
 - In the dialog box, click **Help**.

Readme file

The Readme file contains information about installation and compatibility issues. It also contains technical tips and information about product changes that occurred after this guide went to press. It is installed on your hard disk in the same location as the product files.

To read the Readme file

- 1 In Windows Explorer, double-click **My Computer**.
- 2 Double-click the hard disk on which you installed **Norton AntiVirus Professional**.
In most cases, this will be drive C.
- 3 Click **Program Files > Norton AntiVirus Professional**.
- 4 Double-click **Readme.txt**.
The file opens in Notepad or your default word processing program.
- 5 Close the word processing program when you are done reading the file.

Access the User's Guide PDF

The *Norton AntiVirus Professional User's Guide* is provided on the CD in PDF format. You must have Adobe Acrobat Reader installed on your computer to read the PDF.



If you purchased this product as an electronic download, Adobe Acrobat Reader was not included. You must download it from the Adobe Web site.

To install Adobe Acrobat Reader

- 1 Insert the CD into the CD-ROM drive.
- 2 Click **Browse CD**.

- 3 In the CD window, double-click the **Manual** folder.
- 4 Double-click the **Acrobat** folder.
- 5 Double-click the program file.
- 6 Follow the on-screen instructions to select a folder for Adobe Acrobat Reader and complete the installation.

Once you have installed Adobe Acrobat Reader, you can read the PDF from the CD.



If you do not have a CD, you can download the PDF from the Symantec Service & Support Web site.

To read the User's Guide PDF from the CD

- 1 Insert the CD into the CD-ROM drive.
- 2 Click **Browse CD**.
- 3 Double-click the **Manual** folder.
- 4 Double-click the Norton AntiVirus Professional PDF.

You can also copy a User's Guide to your hard disk and read it from there.

To read a User's Guide from your hard disk

- 1 Open the location into which you copied the PDF.
- 2 Double-click the PDF.

Symantec products on the Web

The Symantec Web site provides extensive information about all Symantec products. There are several ways to access the Symantec Web site.

To access the Web site from the Help menu

- ❖ Select the solution that you want. Your options are:

Symantec Security Response	Takes you to the Security Response page of the Symantec Web site, from which you can update your protection and read the latest information about antithreat technology.
More Symantec solutions	Takes you to the Symantec Store Web site, from which you can get product information on every Symantec product.

Within your Symantec product, the Reports page contains a link to the Symantec online Virus Encyclopedia, as does the Windows Explorer toolbar.

To access the Web site from the Reports page

- 1 In the main window, under Norton AntiVirus, click **Reports**.
- 2 On the Reports page, next to Online Virus Encyclopedia, click **View Report**.

To access the Symantec Web site from Windows Explorer

- 1 Open Windows Explorer.
- 2 On the toolbar, on the Norton AntiVirus menu, click **View Virus Encyclopedia**.
This option connects you to the Symantec Security Response Web page, from which you can search for information on all types of viruses.

To access the Symantec Web site in your browser

- ❖ On the Internet, go to www.symantec.com

Subscribe to the Symantec Security Response newsletter

Each month, Symantec publishes a free electronic newsletter that is focused on the needs of Internet security customers. It discusses the latest antivirus technology produced by Symantec Security Response, common viruses, trends in virus workings, virus outbreak warnings, and special *virus definitions* releases.

To subscribe to the Symantec Security Response newsletter

- 1 On the Internet, go to securityresponse.symantec.com
- 2 On the security response Web page, scroll down to the reference area of the page, then click **Newsletter**.
- 3 On the security response newsletter Web page, select the language in which you want to receive the newsletter.
- 4 On the subscribe Web page, type the information requested, then click **Subscribe**.



The default settings for this product provide complete protection for your computer. However, you may want to adjust them to optimize system performance or disable options that do not apply. You can change the product's settings to fit your work environment.

If you are using Windows 2000/XP, you will need administrator access to change options. If you are an administrator and share your computer with others, keep in mind that the changes that you make apply to everyone using the computer.

Customize Norton AntiVirus

The default settings for Norton AntiVirus provide complete virus protection for your computer. However, you may want to adjust them to optimize system performance or disable options that do not apply.

Norton AntiVirus provides password protection for your option settings. You can enable, change, and reset a password so that unauthorized users cannot tamper with your settings.

All of the options are organized into three main categories. The options contained under each category are as follows.

Category	Options
System	Auto-Protect Manual Scan
Internet	Email Instant Messenger LiveUpdate
Other	Threat Categories Inoculation (Windows 98/98SE/Me) Miscellaneous Advanced Tools

This section does not describe how to change the individual options, but gives a general description of what they do and how you can find them. For specific information about a particular option, check the online Help.

About System options

The System options control scanning and monitoring of your computer. You use System options to determine what gets scanned, what the scan is looking for, and what

happens when a virus or virus-like activity is encountered.

With higher levels of protection, there can be a slight trade-off in computer performance. If you notice a difference in your computer's performance after installation, you may want to set protection to a lower level or disable those options that you do not need.

The System options that you can set are as follows.

Option	Description
Auto-Protect	<p>Determine if Auto-Protect starts when you start your computer, what it looks for while monitoring your computer, and what to do when a virus is found.</p> <p>Auto-Protect options also include Bloodhound, Advanced, and Exclusions subcategories.</p> <ul style="list-style-type: none">■ Bloodhound is the scanning technology that protects against unknown viruses. Use these options to set its level of sensitivity in Auto-Protect.■ Advanced options determine the activities to be monitored when scanning for virus-like activities and when scanning floppy disks.■ Exclusions specify the files that should not be scanned by file name extension or by specific file name. Be careful not to exclude the types of files that are more likely to be infected by viruses such as files with macros or executable files.
Manual Scan	<p>Determine what gets scanned and what happens if a virus or threat is found during a scan that you request.</p> <p>Manual Scan options also include Bloodhound and Exclusions subcategories.</p>

About Internet options

Internet options define what happens when your computer is connected to the Internet. You use Internet options to define how Norton AntiVirus should scan email and instant messenger attachments, enable Worm Blocking, and determine how updates should be applied with LiveUpdate.

The Internet options you can set are as follows.

Option	Description
Email	Enable email scanning and Worm Blocking, and define how Norton AntiVirus should behave while scanning email messages. Scanning incoming email messages protects your computer against viruses sent by others. Scanning outgoing email messages prevents you from inadvertently transmitting viruses or worms to others. You can choose to scan incoming or outgoing email messages, or both, and to display an icon or progress indicator while scanning. You can set options to automatically repair, quarantine, or delete infected email messages with or without interaction with you. Advanced options determine what to do when scanning email messages.
Instant Messenger	Determine what instant messengers to support, how to configure a new instant messenger, and what happens if a virus is found during an instant messenger session.
LiveUpdate	Enable Automatic LiveUpdate and define how updates should be applied. Automatic LiveUpdate checks for updated virus definitions automatically when you are connected to the Internet.

About Other options

Other options include Inoculation settings for Windows 98/98SE/Me and Miscellaneous settings. You can enable Inoculation, cause an alert if a system file changes, set a variety of miscellaneous options, and customize behavior for the Norton Protected Recycle Bin.

The Other options that you can set are as follows.

Option	Description
Threat Categories	Determine the threats that you want Norton AntiVirus to detect. Advanced options include how to respond when a threat is found and what to do when deleting threats. Exclusions options specify the files that should not be scanned by file name extension or by specific file name.
Inoculation	Enable Inoculation and, if a system file changes, choose to update the Inoculation snapshot or repair the file by restoring it to its original values. Inoculation options are available only on Windows 98/98SE/Me.
Miscellaneous	Back up file in Quarantine before attempting a repair. (This option is automatically set to On.) Enable Office Plug-in. If you upgrade to Microsoft Office 2000 or later after Norton AntiVirus is installed, you must enable this option to automatically scan Microsoft Office files. Alert me if my virus protection is out of date. Scan files at system startup (Windows 98/98SE only). Enable password protection for options.
Advanced Tools	Customize the behavior and name of the desktop icon for the Norton Protected Recycle Bin. Enable or disable and customize Norton Protection for deleted files.

Set Norton AntiVirus options

You change the settings for Norton AntiVirus options in the Options window.



If you set a password for Options, Norton AntiVirus asks you for the password before you can continue.

To change settings

- 1 In the main window, click **Options**.
If a menu appears, click **Norton AntiVirus**.

- 2 In the Options window, in the left pane, select an option in the list.
Options with an arrow to the left have sub-options. As you select an option, the corresponding settings for the selected option appear in the right pane.
- 3 Select any settings that you want to change.
- 4 Click **OK**.
These settings now take precedence over the preset options. The changes take effect immediately.

If you need to restore default Norton AntiVirus settings

You can change any or all of the options listed. If you have made a number of changes that have unwanted results, you can restore all options to the default settings.



If you set a password for Options, Norton AntiVirus asks you for the password before you can view or adjust the settings.

To restore default settings on an Options page

- ❖ On the page for which you want to restore default settings, click **Page Defaults**.

To restore default settings for all options

- ❖ On any page in the Options window, click **Default All**.

Password protect Norton AntiVirus options

To protect your Norton AntiVirus options from being changed without your permission, you can choose to protect or remove protection from your option settings with a password. If you specify a password, you are asked to enter a password every time that you view the Options window, or temporarily enable or disable Auto-Protect.

If you forget your password, you can reset it from the Help button in the Norton AntiVirus main window. See the online Help for more information about resetting your password.

To specify or remove a password

- 1 Click **Options**.
If a menu appears, click **Norton AntiVirus**.
- 2 In the Options window, under Other, click **Miscellaneous**.
- 3 Check or uncheck **Enable password protection for options**.
- 4 In the password dialog box, type a password.
- 5 Click **OK**.



Keeping current with LiveUpdate

6

Symantec products depend on current information to protect your computer from newly discovered threats. Symantec makes this information available to you through LiveUpdate. Using your Internet connection, LiveUpdate obtains program updates and protection updates for your computer.

Your normal Internet access fees apply when you use LiveUpdate.



If your computer uses Windows 2000/XP, you must have Administrator *access privileges* to run LiveUpdate.

About program updates

Program updates are minor improvements to your installed product. These differ from product upgrades, which are newer versions of entire products. Program updates that have self-installers to replace existing software code are called patches. Patches are usually created to extend operating system or hardware compatibility, adjust a performance issue, or fix bugs.

LiveUpdate automates the process of obtaining and installing program updates. It locates and obtains files from an Internet site, installs them, and then deletes the leftover files from your computer.

About protection updates

Protection updates are files that are available from Symantec that keep your Symantec products up-to-date with the latest anti-threat technology. The protection updates you receive depend on which product you are using.

Norton AntiVirus, Norton AntiVirus Professional, Norton SystemWorks, Norton SystemWorks Professional, Symantec AntiVirus for Handhelds – Annual Service Edition	Users of Norton AntiVirus, Norton SystemWorks, and Symantec AntiVirus for Handhelds – Annual Service Edition products receive virus protection updates, which provide access to the latest virus signatures and other technology from Symantec.
Norton Internet Security, Norton Internet Security Professional	<p>In addition to the virus protection updates, users of Norton Internet Security products also receive protection updates for Web filtering, intrusion detection, and Norton AntiSpam.</p> <p>The Web filtering protection updates provide the latest lists of Web site addresses and Web site categories that are used to identify inappropriate Web content.</p> <p>The intrusion detection updates provide the latest predefined firewall rules and updated lists of applications that access the Internet. These lists are used to identify unauthorized access attempts to your computer.</p> <p>Norton AntiSpam updates provide the latest spam definitions and updated lists of spam email characteristics. These lists are used to identify unsolicited email.</p>
Norton Personal Firewall	Users of Norton Personal Firewall receive intrusion detection updates for the latest predefined firewall rules and updated lists of applications that access the Internet.
Norton AntiSpam	Users of Norton AntiSpam receive the latest spam definitions and updated lists of spam email characteristics.

Obtain updates using LiveUpdate

LiveUpdate checks for updates to all of the Symantec products that are installed on your computer.



If your *Internet service provider* does not automatically connect you to the Internet, connect to the Internet first, and then run LiveUpdate.

To obtain updates using LiveUpdate

- 1 At the top of the main window, click **LiveUpdate**.
- 2 In the LiveUpdate window, click **Next** to locate updates.
- 3 If updates are available, click **Next** to download and install them.
- 4 When the installation is complete, click **Finish**.



Some program updates may require that you restart your computer after you install them.

When you should update

Run LiveUpdate as soon as you have installed your product. Once you know that your files are up-to-date, run LiveUpdate regularly to obtain updates. For example, to keep your virus protection current, you should use LiveUpdate once a week or whenever new viruses are discovered. Program updates are released on an as-needed basis.

If you can't use LiveUpdate

When new updates become available, Symantec posts them on the Symantec Web site. If you can't run LiveUpdate, you can obtain new updates from the Symantec Web site.

To obtain updates from the Symantec Web site

- 1 Point your Web browser to securityresponse.symantec.com
- 2 Follow the links to obtain the type of update that you need.

Set LiveUpdate to Interactive or Express mode

LiveUpdate runs in either Interactive or Express mode. In Interactive mode (the default), LiveUpdate *downloads* a list of updates that are available for your Symantec products that are supported by LiveUpdate technology. You can then choose which updates you want to install. In Express mode, LiveUpdate automatically installs all available updates for your Symantec products.

To set LiveUpdate to Interactive or Express mode

- 1 At the top of the main window, click **LiveUpdate**.
- 2 In the LiveUpdate welcome screen, click **Configure**.
- 3 In the LiveUpdate Configuration dialog box, on the General tab, select the mode that you want. Your options are:

Interactive Mode	Gives you the option of choosing which updates you want to install
Express Mode	Automatically installs all available updates

- 4 If you selected Express Mode, select how you want to start checking for updates. Your options are:

I want to press the start button to run LiveUpdate	Gives you the option of cancelling the update
I want LiveUpdate to start automatically	Installs updates automatically whenever you start LiveUpdate

- 5 To have access to a Symantec self-help Web site in the event that an error occurs while using LiveUpdate, check **Enable Enhanced Error Support**.
- 6 Click **OK**.

Turn off Express mode

Once you have set LiveUpdate to run in Express mode, you can no longer access the LiveUpdate Configuration dialog box directly from LiveUpdate. You must use the Symantec LiveUpdate control panel.

To turn off Express mode

- 1 On the Windows taskbar, click **Start > Settings > Control Panel**.
- 2 In the Control Panel window, double-click **Symantec LiveUpdate**.
- 3 In the LiveUpdate Configuration dialog box, on the General tab, click **Interactive Mode**.
- 4 Click **OK**.

If you run LiveUpdate on an internal network

If you run LiveUpdate on a computer that is connected to a network that is behind a company firewall, your network administrator might set up an internal LiveUpdate server on the network. LiveUpdate should find this location automatically.

If you have trouble connecting to an internal LiveUpdate server, contact your network administrator.

Run LiveUpdate automatically

You can have LiveUpdate check for protection updates automatically, on a set schedule, by enabling Automatic LiveUpdate. You must continue to run LiveUpdate manually to receive product updates.



Automatic LiveUpdate checks for an Internet connection every five minutes until a connection is found, and then every four hours. If you have an ISDN *router* that is set to automatically connect to your *Internet service provider* (ISP), many connections will be made, with connection and phone charges possibly being incurred for each connection. If this is a problem, you can set your ISDN router to not automatically connect to the ISP or disable Automatic LiveUpdate.

To enable Automatic LiveUpdate

- 1 At the top of the main window, click **Options**.
If a menu appears, click **Norton AntiVirus**.



- If you set a password for Options, you must provide the password before you can continue.
- 2 In the Options window, under Internet, click **LiveUpdate**.
 - 3 In the LiveUpdate pane, check **Enable Automatic LiveUpdate**.

- 4 Set how you want updates to be applied. Your options are:

Apply updates without interrupting me	LiveUpdate checks for and installs protection updates without prompting you. LiveUpdate displays an alert when a protection update has been downloaded. You should still run LiveUpdate occasionally to check for program updates.
Notify me when updates are available	LiveUpdate checks for protection updates and asks if you want to install them.

- 5 Click **OK**.

To delete the schedule for Automatic LiveUpdate, disable Automatic LiveUpdate.

To disable Automatic LiveUpdate

- 1 At the top of the main window, click **Options**.
If a menu appears, click **Norton AntiVirus**.
- 2 In the Options window, under Internet, click **LiveUpdate**.
- 3 In the LiveUpdate pane, uncheck **Enable Automatic LiveUpdate**.
- 4 Click **OK**.



If you set a password for Options, you must provide the password before you can continue.

About your subscription

See ["About protection updates"](#) on page 70.

Your Symantec product includes a complimentary, limited-time subscription to protection updates that are used by your product. When the subscription is due to expire, you are prompted to renew your subscription.

If you do not renew your subscription, you can still use LiveUpdate to obtain program updates. However, you cannot obtain protection updates through LiveUpdate or from the Symantec Web site and will not be protected against newly discovered [threats](#). Also, whenever you use LiveUpdate, you will receive a warning that your subscription has expired. Follow the on-screen instructions to complete your subscription renewal.

Protecting disks, files, and data from viruses

7

Keeping your computer protected requires regular monitoring by Auto-Protect and Worm Blocking; scanning of your email attachments and files transferred by instant messenger; and frequent system scans. All of these tasks can be set to occur automatically.

For added protection in Norton AntiVirus on Windows 98/98SE/Me, enable Inoculation to alert you if a system file changes.

Ensure that protection settings are enabled

Norton AntiVirus is configured to provide you with complete protection against viruses. It is unlikely that you need to change any settings. However, for maximum protection, you should ensure that your protection features are enabled.



For specific information about a particular option and its protection settings, see the online Help.

This table summarizes the maximum protection settings and where you can find them.

Feature	In the main window, click	Then for maximum protection, select
Auto-Protect	Enable	On
Email scanning	Options > Email	<ul style="list-style-type: none"> ■ Scan incoming Email ■ Scan outgoing Email <p>If your email program uses one of the supported communications protocols, both options are selected by default.</p>
Timeout protection	Options > Email	<p>Protect against timeouts when scanning Email</p> <p>To prevent connection timeouts while receiving large attachments, enable timeout protection.</p>
Instant messenger scanning	Options > Instant Messenger	Instant messengers that you want to protect
Worm Blocking	Options > Email	<ul style="list-style-type: none"> ■ Enable Worm Blocking ■ Alert me when scanning email attachments
Inoculation (Windows 98)	Options > Inoculation	Inoculate Boot Records

Manually scan disks, folders, and files

If Auto-Protect is enabled and the Norton AntiVirus options are set at their default levels, you normally would not need to scan manually. However, if you temporarily disabled Auto-Protect (for example, to load or use another program that conflicts with Norton AntiVirus), and you forgot to enable it again, it is possible that a virus could be on your hard disk undetected. You can scan your entire computer, or individual floppy disks, drives, folders, or files.

Although the default settings for manual scanning are usually adequate, you can raise the level of Bloodhound heuristics or adjust the options for manual scanning in the Options window.

For more information about manual scanning options, see the online Help.

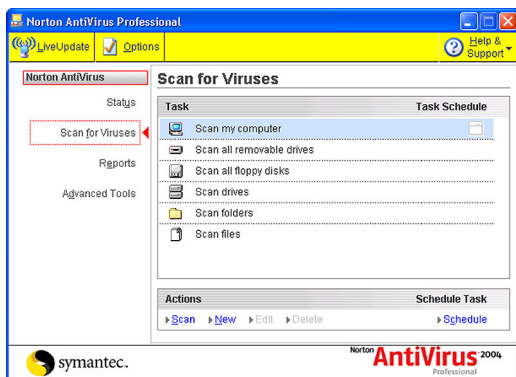
Perform a full system scan

A full system scan scans all *boot records* and files on your computer.

To perform a full system scan

- 1 On the left side of the main window, under Norton AntiVirus, click **Scan for Viruses**.

- 2 In the Scan for Viruses pane, under Task, click **Scan my computer**.



- 3 Under Actions, click **Scan**.
When the scan is complete, a scan summary appears.
- 4 When you are done reviewing the summary, click **Finished**.

Scan individual elements

Occasionally, you may want to scan a particular file, removable drives, a floppy disk, any of your computer's drives, or any folders or files on your computer. You may have been working with floppy disks or have received a compressed file in an email message and suspect a virus. You can scan just a particular disk or individual element that you want to check.

To scan individual elements

- 1 On the left side of the main window, under Norton AntiVirus, click **Scan for Viruses**.
- 2 In the Scan for Viruses pane, under Task, select the scan that you want to run.
- 3 Under Actions, click **Scan**.
If you choose to scan all removable drives or a floppy disk, the scan starts automatically. If you choose to scan drives, folders, or files, a dialog box appears in

which you choose which drives, folders, or files to scan.

- 4 In the dialog box, make your selection, then click **Scan**.

When the scan is complete, a scan summary appears.

- 5 When you are done reviewing the summary, click **Finished**.

If problems are found during a scan

See ["What to do if a virus is found"](#) on page 87.

At the end of a scan, a summary report appears to tell you what Norton AntiVirus found during the scan. If a virus was found and you have requested that Norton AntiVirus repair the file automatically, it is listed as repaired. If the file cannot be repaired, it can be quarantined or deleted.

Create and use custom scans

See ["Schedule a custom scan"](#) on page 84.

You can create a custom scan if you regularly scan a particular segment of your computer and don't want to have to specify the segment to be scanned every time. You can also schedule the custom scan to run automatically.

You can delete the scan when it is no longer necessary. For example, if you are working on a project for which you need to frequently swap files with others, you might want to create a folder into which you copy and scan those files before using them. When the project is done, you can delete the custom scan for that folder.

To create a custom scan

- 1 On the left side of the main window, under Norton AntiVirus, click **Scan for Viruses**.
- 2 In the Scan for Viruses pane, under Actions, click **New**.
- 3 In the opening window of the Norton AntiVirus Scan Wizard, click **Next**.

- 4 Select the items that you want to scan. Your options are:

Add files	Select individual files to be scanned.
Add folders	Select folders and drives to be scanned.

You can use both options to select the combination of items that you want.

- 5 In the resulting dialog box, select the items that you want to scan.
If you select a folder, all files in that folder are included. If you select a drive, all folders and files on that drive are included.
- 6 Add the selected items to the list of items to scan by doing one of the following:
 - In the Scan Files dialog box, click **Open**.
 - In the Scan Folders dialog box, click **Add**.
- 7 If you need to remove an item from the list, select it, then click **Remove**.
- 8 When you are done creating the list of items to be scanned, click **Next**.
- 9 Type a name for the scan by which you can identify it in the list of scans.
- 10 Click **Finish**.

Run a custom scan

When you run a custom scan, you do not have to redefine what you want to scan.

To run a custom scan

- 1 On the left side of the main window, under Norton AntiVirus, click **Scan for Viruses**.
- 2 In the Scan for Viruses pane, under Task, select the custom scan.
- 3 Under Actions, click **Scan**.
When the scan is complete, a scan summary appears.
- 4 When you are done reviewing the summary, click **Finished**.

Delete a custom scan

You can delete custom scans if they are no longer needed.

To delete a custom scan

- 1 On the left side of the main window, under Norton AntiVirus, click **Scan for Viruses**.
- 2 In the Scan for Viruses pane, under Task, select the custom scan that you want to delete.



If you click the button next to the scan name, the scan runs.

- 3 Under Actions, click **Delete**.
- 4 Click **Yes** to verify that you want to delete the scan.

Schedule scans

After installation, Norton AntiVirus automatically runs a weekly full system scan. You can also set up a schedule for custom virus scans.

You can schedule customized virus scans that run unattended on specific dates and times or at periodic intervals. If you are using the computer when the

scheduled scan begins, it runs in the background so that you do not have to stop working.



You cannot schedule the predefined scans in the scan list, but you can schedule any custom scans that you have created.

Schedule a custom scan

You have complete flexibility in scheduling custom scans. When you select how frequently you want a scan to run (such as daily, weekly, or monthly), you are presented with additional fields with which you can refine your request. For example, you can request a daily scan, then schedule it to occur every two days or every three days instead.

To schedule a custom scan

- 1 On the left side of the main window, under Norton AntiVirus, click **Scan for Viruses**.
- 2 In the Scan for Viruses pane, under Task, select the custom scan that you want to schedule.



If you click the button next to the scan name, the scan runs.

- 3 Under Schedule Task, click **Schedule**.
- 4 In the Schedule dialog box, if Show multiple schedules is checked, click **New** to enable the scheduling fields.
If it is not checked, the fields are already enabled.
- 5 Set the frequency and time at which you want the scan to run.
Most of the frequency options include additional options that let you further refine the schedule. Set the additional options as necessary.
- 6 When you are done, click **OK**.

You can also create multiple schedules for a scan. For example, you could run the same scan at the beginning of your work day and at the end.

To create multiple schedules for a single scan

- 1 On the left side of the main window, under Norton AntiVirus, click **Scan for Viruses**.
- 2 In the Scan for Viruses pane, under Task, select the custom scan that you want to schedule.



If you click the button next to the scan name, the scan runs.

- 3 Under Schedule Task, click **Schedule**.
- 4 In the Schedule dialog box, check **Show multiple schedules**.
- 5 To set an additional schedule, click **New**.
- 6 Set the frequency and time at which you want the scan to run.
Most of the frequency options include additional options that let you further refine the schedule. Set the additional options as necessary.
- 7 When you are done, click **OK**.

Edit scheduled scans

You can change the schedule of any scheduled scan, including the weekly full system scan.

To edit a scheduled scan

- 1 On the left side of the main window, under Norton AntiVirus, click **Scan for Viruses**.
- 2 In the Scan for Viruses pane, under Task, select the scan that you want to reschedule.



If you click the button next to the scan name, the scan runs.

- 3 Under Schedule Task, click **Schedule**.
- 4 Change the schedule as desired.
- 5 Click **OK**.

Delete a scan schedule

You can delete any scan schedule. Deleting the schedule does not delete the scan.

To delete a scan schedule

- 1 On the left side of the main window, under Norton AntiVirus, click **Scan for Viruses**.
- 2 In the Scan for Viruses pane, under Task, select the scan whose schedule you want to delete.



If you click the button next to the scan name, the scan runs.

- 3 Under Schedule Task, click **Schedule**.
- 4 In the Schedule dialog box, check **Show multiple schedules**.
- 5 Select the schedule or schedules that you want to delete.
- 6 Click **Delete**.
- 7 Click **OK**.

What to do if a virus is found

8



If after reviewing the information in this chapter, you have not resolved your problem, see “[Responding to emergencies](#)” on page 11 and “[Troubleshooting](#)” on page 107.

If Norton AntiVirus finds a virus or a file containing a virus or a potential security risk on your computer, there are several possible resolutions to the problem:

- **Fix infection**
Removes the virus from the file or if the threat is a worm or Trojan horse, deletes the file.
- **Quarantine infection**
Makes the file inaccessible by any programs other than a Symantec antivirus program. You cannot accidentally open the file and spread the virus, but you can still evaluate it for possible submission to Symantec.
- **Delete the file**
Removes the virus from your computer by deleting the file that contains the virus, worm, or Trojan horse. It should be used only if the file cannot be repaired or quarantined.
- **Exclude at-risk files**
Excludes the files at risk from future scans. If you exclude a file, you are doing so permanently from future scans. The threat may still be on your computer.

See “[If Norton AntiVirus places files in Quarantine](#)” on page 93.

Viruses can be found during a manual or scheduled scan or by Auto-Protect when you perform an action with an

infected file. Threats and security risks can appear during an instant messenger session, when sending an email message, or during a manual or scheduled scan.

If a virus is found during a scan

If Norton AntiVirus finds a virus, Trojan horse, worm, or security risk during a scan or from an instant messenger session, you either receive a summary of the automatic repair or deletion results, or use the Repair Wizard to resolve the problem.

Review the repair details

If you have set your manual scan options so that Norton AntiVirus repairs or deletes files automatically, and all infected files could be repaired or deleted, the scan summary lists the number of files found, infected, and repaired or deleted. This information is presented for status purposes only; you don't need to take further action to protect your computer. If you want to know more, you can check the repair details to see which files were infected and with which [threats](#).

To review the repair details

- 1 In the scanner window, in the Summary pane, click **More Details**.
- 2 When you are done reviewing the results, click **Finished**.

Use the Repair Wizard

If there are files that could not be fixed, or if you have set options so that Norton AntiVirus asks you what to do when a virus or threat is found, the Repair Wizard opens. If Norton AntiVirus did not attempt a repair, the Repair Wizard opens in the Fix Infection pane. Otherwise, it opens in the Quarantine window.

To use the Repair Wizard

- 1 If the Repair Wizard opens in the Fix Infections pane, uncheck any files that you don't want Norton

AntiVirus to fix.

All files are checked by default. This is the recommended action.

2 Click **Fix.**

If any files cannot be fixed or deleted, the Quarantine Infections window opens. All files are checked to be added to Quarantine by default. This is the recommended action.

3 In the Quarantine window, uncheck any files that you do not want to quarantine.

4 Click **Quarantine.**

If any files could not be quarantined, the Delete window opens. All files are checked to be deleted by default.

5 In the Delete window, uncheck any files that you do not want to delete.



If you do not delete the infected files, the virus or file at risk remains on your computer and can cause damage or be transmitted to others.

6 Click **Delete.**

If any files could not be deleted, the Exclude At-risk Files window opens to allow you to exclude files considered to be at risk from future scans.

7 In the Exclude At-risk Files window, select any files that you want to exclude.

8 Click **Exclude.**

9 Once all of the files have been repaired, quarantined, deleted, or excluded, the Scan Summary window opens.



If any files could not be deleted, they appear in the Scan Summary window with a status of at risk or delete failed. There are a variety of reasons why some files cannot be deleted: a file could be in use or part of a larger program. Norton AntiVirus recommends that you select the threat name to review the information from the Internet and determine the appropriate action.

10 When you are done reviewing the summary, click **Finished.**

If a virus is found by Auto-Protect

See ["Ensure that protection settings are enabled"](#) on page 77.

Auto-Protect scans files for viruses when you perform an action with them, such as moving them, copying them, or opening them. If it detects a virus or virus-like activity, in most cases you receive an [alert](#) telling you that a virus was found and repaired. How you proceed depends on the operating system that you are using.

If you are using Windows 98/98SE/Me

If a virus or threat is found and repaired by Auto-Protect in Windows 98/98SE/Me, you receive an [alert](#) telling you which file was repaired or deleted.

To close the alert

- ❖ Click **Finish**.

If you have set your options so that Auto-Protect asks you what to do when it finds a virus, the alert asks you to choose one of the following actions. The recommended action is always preselected.

Action	Result
Repair the infected file	Automatically eliminates the virus, Trojan horse, or worm and repairs or deletes the infected file. When a virus is found, Repair is always the best choice.
Quarantine the infected file	Isolates the infected file, but does not remove the threat. Select Quarantine if you suspect that the infection is caused by an unknown threat and you want to submit the threat to Symantec for analysis.
Delete the infected file	Erases both the threat and the infected file. Select Delete if Repair is not successful. Replace the deleted file with the original program file or backup copy. If the virus, Trojan horse, or worm is detected again, your original copy is infected.
Do not open the file, but leave the problem alone	Stops the current operation to prevent you from using an infected file. This action does not solve the problem. You will receive an alert the next time that you perform the same activity.

Action	Result
Ignore the problem and do not scan this file in the future	Adds the file that is suspected of containing a threat to the Exclusions list. When you add a file to the Exclusions list, the file is excluded from any future virus scans, unless you remove it from the list. Select this option only if you know that the file does not contain a virus.
Ignore the problem and continue with the infected file	Continues the current operation. Select this option only if you are sure that a virus, Trojan horse, or worm is not at work. You will receive an alert again. If you are not sure what to do, select Do not open the file, but leave the problem alone.

If a file cannot be repaired, you receive an alert telling you that the repair was not made and recommending that you quarantine the file. You have the same options as those listed in the table, with the exception of Repair the infected file.

If you are using Windows 2000/XP

If a virus is found and either repaired or automatically deleted by Auto-Protect in Windows 2000/XP, you receive an [alert](#) telling you which file was repaired or deleted and which virus, Trojan horse, or worm was infecting the file. If you have an active Internet connection, selecting the virus name opens the Symantec Web page that describes the virus.

To close the alert

❖ Click **OK**.

If the file cannot be repaired, you receive two alerts, one telling you that Auto-Protect was unable to repair the file, and another telling you that access to the file was denied.

You can set your Auto-Protect options to try to quarantine any infected files that it cannot repair. If you do this, you are informed if any files are quarantined.

To resolve problems with unrepaired files

- 1 Run a full system scan on your computer to ensure that no other files are infected.

See [“If Norton AntiVirus places files in Quarantine”](#) on page 93.

- See "If a virus is found during a scan" on page 88.
- 2 Follow the recommended actions in the Repair Wizard to protect your computer from the infected files.

If a threat is found by Worm Blocking

See "Ensure that protection settings are enabled" on page 77.

If a program tries to email itself or email a copy of itself, it could be a worm trying to spread via email. A *worm* can send itself or a copy of itself in an email message without any interaction with you.

Worm Blocking continually scans outgoing email attachments for worms. If it detects a worm, you receive an *alert* telling you that a malicious worm was found.

The alert presents you with options and asks you what to do. If you were not sending an email message at that time, then it is probably a worm and you should quarantine the file. You can click Help on the alert for additional information about how to respond.

After you have responded to the *threat* and deleted the file, you could still have an infected system. Follow these procedures.

Procedure	For more information
Run LiveUpdate to ensure that you have the latest protection updates.	See "About protection updates" on page 70.
Scan your system.	See "Perform a full system scan" on page 79.
Go to the Symantec Security Response Web page for the most up-to-date virus definitions and clean-up tools.	See the Symantec Security Response Web page at securityresponse.symantec.com

If Inoculation alerts you about a change in system files



See ["Ensure that protection settings are enabled"](#) on page 77.

Inoculation protection is available on Windows 98/98SE/Me systems only.

System files can change for a variety of reasons. You may have updated your operating system or repartitioned your hard disk, or you could have a virus. Norton AntiVirus alerts you when a change occurs in your system files.

If you get an [alert](#) about a change in your system files, you have two options. You can update your Inoculation snapshot or repair the file. Before you repair the file, be sure that your virus definitions are up-to-date and run a scan.

To respond to Inoculation changes

- ❖ In the Alert window, select the action that you want to take. Your options are:

Update the saved copy of my Master Boot Record	Use if the alert appears after a legitimate change in system files.
Restore my Master Boot Record	Use if you are certain the system did not change for legitimate reasons.

If Norton AntiVirus places files in Quarantine

Once a file has been placed in Quarantine, you have several options. All of the actions that you take on files in Quarantine must be performed in the Quarantine window.

The toolbar at the top of the Quarantine window contains all of the actions that you can perform on quarantined files.

Add Item	Adds files to Quarantine. Use this action to quarantine a file that you suspect is infected. This action has no effect on files that are already in Quarantine.
Properties	Provides detailed information about the selected file and the virus that is infecting it.
Repair Item	Attempts to repair the selected file. Use this action if you have received new virus definitions since the file was added to Quarantine.
Restore Item	Returns the selected file to its original location without repairing it.
Delete Item	Deletes the selected file from your computer.
Submit Item	Sends the selected file to Symantec. Use this option if you suspect that a file is infected even if Norton AntiVirus did not detect it.
LiveUpdate	Runs LiveUpdate to check for new protection and program updates. Use this if you haven't updated your virus definitions for a while and then try to repair the files in Quarantine.

To open the Quarantine window

- 1 On the left side of the main window, under Norton AntiVirus, click **Reports**.
- 2 In the Reports pane, on the Quarantined items line, click **View Report**.

To perform an action on a file in Quarantine

- 1 In the Quarantine window, select the file on which you want to perform the action.
- 2 On the toolbar, select the action that you want to perform.
- 3 When you are finished, on the File menu, click **Exit**.

If Norton AntiVirus cannot repair a file

See “[Keeping current with LiveUpdate](#)” on page 69.

One of the most common reasons that Norton AntiVirus cannot automatically repair or delete an infected file is that you do not have the most up-to-date virus definitions. Update your virus definitions with LiveUpdate and scan again.

If that does not work, read the information in the report window to identify the types of items that cannot be repaired, and then take one of the following actions, depending on the file type.

File type	Action
Infected files with .exe, .doc, .dot, or .xls file name extensions (any file can be infected)	Use the Repair Wizard to solve the problem. For more information, see the online Help.
Hard disk master boot record, boot record, or system files (such as IO.SYS or MSDOS.SYS) and floppy disk boot record and system files	Replace using the Rescue Disks or your operating system disks. For more information, see the online Help.

Look up viruses on the Symantec Web site

The Symantec Web site contains a complete list of all known viruses and related malicious code, along with descriptions. You must be connected to the Internet to look up viruses.

To look up viruses

- 1 On the left side of the main window, under Norton AntiVirus, click **Reports**.
- 2 In the Reports pane, on the Online Virus Encyclopedia line, click **View Report**.
The Symantec Web site opens in your Internet browser.
- 3 Use the links on the Web page to access the virus information for which you are looking.

Recovering missing or erased files

9



If you purchased this product to recover files, do not install it and do not start Windows. Any new files copied to your hard disk might overwrite existing data. Starting Windows writes to your hard disk. The Windows swap file could overwrite data you would like to recover.

See [“About Rescue Disks”](#) on page 49.

When you erase a file using Windows Explorer, Windows keeps a temporary copy of the file in the Recycle Bin. However, Windows does not detect files that were erased or overwritten by applications running in Windows, erased from a command prompt, or deleted via a permanent method, such as using Shift+Delete.

About Norton Protection

The Norton Protected Recycle Bin protects the following types of files:

- Files that are deleted while you are using the command line
- Files that are created and deleted by Windows applications
- Older versions of files that you modify and overwrite
- Files that were deleted by viruses or other malicious threats, if they use a standard Windows or DOS deletion method
- If the standard Windows Recycle Bin is not enabled, files that would otherwise be under Recycle Bin protection

Files that are shared on a network or stored on a network server and files deleted while using your computer in DOS mode rather than Windows are not protected.



Windows 2000/XP operating systems only track ownership and rights on NTFS volumes. With NTFS volumes, you are told how many files are yours before you purge them. If you delete a file on an FAT/FAT32 drive, the system does not differentiate between your files and those belonging to another user. When you purge your files, the system also purges all of the files to which the other user has access, which includes all files on FAT/FAT32 volumes.

About UnErase Wizard

UnErase Wizard helps you recover deleted files from the Norton Protected Recycle Bin. In Windows 98/Me, UnErase Wizard can also help you restore files that were unprotected by Norton Protection. Windows 2000/XP can only recover files if Norton Protection is turned on.

UnErase Wizard also helps you recover files that are deleted from the standard Windows Recycle Bin. In Windows 98/Me, UnErase Wizard frequently recovers unprotected files as well, even those deleted from the Recycle Bin.



If you have a dual boot system and the volume containing deleted files is not NTFS, you can use the Windows 98/Me version of UnErase Wizard to recover deleted files.

See ["Recover a file with UnErase Wizard"](#) on page 98.

Using UnErase Wizard, you can search for a deleted file by its file name and by words that you think the file may contain. This is especially useful if you can't remember the file name, but you do remember its contents.

Recover a file with UnErase Wizard



If you have excluded files from Norton Protection and these excluded files are deleted, they are not intercepted by the Windows Recycle Bin or Norton Protection and

therefore are not recoverable on Windows 2000/XP systems.

UnErase Wizard displays a list of deleted files or the files that conform to file name criteria that you provide. Each file is described by its name, original location, the date it was deleted, *file type*, file size, and the program that was used to delete it. You can view the contents of a file before or after you recover it.

To see if a file is recoverable

- 1 In the center of the file list, right-click, then click **Show Unrecoverable Files**.
- 2 Click **Next**.
 Use the UnErase Wizard pages to search for and recover the files.

To recover a file with UnErase Wizard

- 1 In the main window, click **Advanced Tools**.
- 2 On the UnErase Wizard line, click **Start Tool**.
- 3 In the UnErase Wizard dialog box, select the action that you want to take. Your options are:

Find recently deleted files	Searches for the names of the most recently deleted files and displays up to a maximum of 25 deleted files (Windows 98/Me only).
Find all protected files on local drives	Searches for and displays the names of all deleted files that are protected by Norton Protection or the Windows Recycle Bin on your computer.
Find any recoverable files matching your criteria	Prompts you for search criteria. Use this option if you are looking for words that are contained in a deleted file.
Find all Norton Protected Users files	Searches for other users' protected files as well as your own. (This option is available only in Windows 2000/XP.)

- 4 Click **Next**.
UnErase Wizard displays a list of the most recently deleted files.
- 5 Select the file that you want to recover.
- 6 Click **Recover**.
If you want to examine the recovered file, make a note of the recovery destination.
- 7 If you are using Windows 98/Me and your deleted file is not listed, click **Next**.
UnErase Wizard guides you through the process of creating a more complete list of deleted files from which to select.
- 8 To close UnErase Wizard, click **Finish**.



A recovered file's name might have a question mark (?) in place of the first letter. If so, you are prompted to type the first letter of the original file name. If you do not know what it is, type any letter from A to Z as a substitute. Make a note of the file name so that you can find it later.

If you delete a file on a floppy disk from a DOS prompt by specifying file name letters after a wildcard (such as DEL *ILENAME.TXT as opposed to DEL FILENAME.TXT or DEL *.TXT), the file is listed as unrecoverable on the Recently Deleted Files page.

Eliminating data permanently

10



Wipe Info lets you remove selected files or folders from your hard disk.

If you are running a recovery application such as System Restore or Norton GoBack, you must erase your history before running Wipe Info to ensure that the data is completely wiped.

About Wipe Info

Wipe Info Wizard erases files or folders from your hard disk so that they cannot be recovered.

When you wipe a file, Wipe Info wipes the file and attempts to wipe any free space that is associated with the file and the file's directory entry.

When you wipe a folder, Wipe Info wipes all of the files in the folder, and then, if the folder is empty, it attempts to wipe the directory entry for the folder.

In general, you cannot recover files that have been wiped. Windows Me/XP System Restore can restore files that have been wiped if they are one of the protected file types. By default, many document types, such as .doc and .xls files in My Documents, are protected. Windows Me/XP System Restore maintains copies of protected files. Wiping the original file does not wipe the copy that Windows Me/XP System Restore maintains.

Wipe Info eliminates a file's contents from the disk, but does not remove the file name. While the file name

remains on disk, it is no longer visible in Windows Explorer, and there is no data stored with it. On NTFS volumes, streams (alternate data that belongs to a file but is not stored with the file) are also wiped.



Never store sensitive information in a file name or attribute. This data can be replicated throughout your system without your knowledge, for example, in a list of most recently used files, or a file name search. This type of embedded information can be very difficult to remove from your computer.

About hexadecimal values

Wipe Info uses hexadecimal values to wipe files. Hexadecimal refers to the base 16 number system. This system is used by computer programmers to represent numbers in the binary number system, which uses the zero and one symbols in combinations to represent any number.

The hexadecimal system consists of the numbers 0 to 9 and the letters A to F, used in combinations. For example, the decimal number 14 is represented as the letter E in the hexadecimal system.

In Wipe Info options, you can specify values from 00 to FF, representing numbers from 0 to 255 respectively. You can type the value using a number or a character from A to F.

About the Government Wipe process

When you select Government Wipe, Wipe Info does the following:

- Overwrites the data with 00s
- Verifies the 00 overwrite
- Overwrites with FFs
- Verifies the FF overwrite
- Writes a random value, or a value that you choose from 00 to FF
- Verifies the random overwrite

- Reverifies the random overwrite to ensure that it was written correctly
- Repeats as many times as you specify, up to 100

Set Wipe Info options

You can specify how Wipe Info handles hidden, read-only, and system files. You can also specify the type of wipe to use. The following wiping methods are available.

Fast Wipe	Overwrites the data that is being wiped with the hexadecimal value of your choice
Government Wipe	Combines several wiping and overwriting processes to conform to specifications in DoD (Department of Defense) document 5220-22-M, National Industrial Security Program Operating Manual, for the ultimate security level when eliminating data from digital media See "About the Government Wipe process" on page 102.

To change Wipe Info options

- 1 In the main window, click **Advanced Tools**.
- 2 On the Wipe Info line, click **Start Tool**.
- 3 Click **Options**.
- 4 On the General tab, select the options for Read-only, System, and Hidden file types.
- 5 On the Wipe Type tab, select one of the following:
 - Fast Wipe
 - Government Wipe
- 6 In the Hex Value text box, type the hexadecimal values that Wipe Info should use when it overwrites the wiped files space.
- 7 In the Times to Perform This Wipe text box, type the number of times that Wipe Info should repeat this process.
- 8 Click **Apply**.

See ["About the Government Wipe process"](#) on page 102.

See ["About hexadecimal values"](#) on page 102.

Wipe files or folders

The procedure for wiping a file varies based on the operating system on your computer. To wipe a file or folder in Windows 2000/XP, add it to the Wipe Info window.

To wipe files or folders in Windows 2000/XP

- 1 In the main window, click **Advanced Tools**.
- 2 On the Wipe Info line, click **Start Tool**.
- 3 Click **Wipe Info**.
- 4 In the Wipe Info window, click **Browse**.
- 5 Select one of the following:
 - Folders
 - Files
- 6 Select the folder or file to wipe.
- 7 Click **Open**.
- 8 With the Wipe Info window open, locate a folder or file on your hard disk.
- 9 Drag the selected item into the Wipe Info file list.
- 10 Continue to drag all of the files and folders that you want to wipe into the Wipe Info list.
If you add an item to the list by mistake, select the item, then right-click **Remove Item(s) from list**.
- 11 Click **Wipe All**.
- 12 Click **Yes** to confirm the warning.
All of the files in the list are wiped.

In Windows 98/Me, Wipe Info uses a wizard to automate the wiping process.

To wipe files or folders in Windows 98/Me

- 1 In the main window, click **Advanced Tools**.
- 2 On the Wipe Info line, click **Start Tool**.
- 3 Click **Wipe Info**.

- 4 In the Wipe Info Wizard window, select one of the following options. Your options are:

Files	Wipe Info deletes the selected file, its directory entry if possible, and any associated free space.
Folders	Wipe Info deletes all files in the selected folder, its directory entry if possible, and any associated free space. You can specify whether subfolders should be included.
Free Space	Wipe Info wipes the free space on the selected disk. This includes free disk space, file slack space, and erased file entries that are not in the Recycle Bin. (You must empty the Recycle Bin to have deleted files wiped.) Wipe Info verifies the disk's integrity before wiping free space.

- 5 Select the file, folder, or disk, then click **Next**.
- 6 If you see a warning message, click **Yes** to proceed.
- 7 For Wipe Options, select one of the following:
- Fast Wipe
 - Government Wipe
- 8 If you want to change any selections, click **Back**. Wipe Info displays its progress and summarizes the results, including any problems that were encountered during the wiping process.
- 9 In the Wipe Summary window, review what Wipe Info will do, then click **Next**.
- 10 View the results, then click **Close**.
- 11 Follow the on-screen instructions to finish the wiping process.

See ["Set Wipe Info options"](#) on page 103.



The information in this chapter will help you solve the most frequently encountered problems. If you can't find the solution to your problem here, there is a wealth of information on the Symantec Web site.

Explore the Symantec service and support Web site

On the Symantec service and support Web site, you can find the latest protection and program updates, patches, online tutorials, Knowledge Base articles, and virus removal tools.

To explore the Symantec service and support Web site

- 1 On the Internet, go to www.symantec.com/techsupp
- 2 On the service and support Web page, under the heading home & home office/small business, click **Continue**.
- 3 On the home & home office/small business page, click **start online support**.
- 4 Follow the links to the information that you want.

If you cannot find what you are looking for using the links on the introduction page, try searching the Web site.

To search the Symantec service and support Web site

- 1 On the left side of any Symantec Web site page, click **search**.
- 2 On the search page, type a word or phrase that best represents the information for which you are looking. Use the following guidelines when searching the Symantec Web site:
 - Type a single word in lowercase letters to find all occurrences of the word, including partial matches. For example, type `install` to find articles that include the word `install`, `installation`, `installing`, and so on.
 - Type multiple words to find all occurrences of any of the words. For example, type `virus definitions` to find articles that include `virus` or `definitions` or both.
 - Type a phrase enclosed in quotation marks to find articles that include this exact phrase.
 - Type a plus (+) sign in front of all of the search terms to retrieve documents containing all of the words. For example, `+Internet +Security` finds articles containing both words.
 - For an exact match, type the search words in uppercase letters.
 - To search for multiple phrases, enclose each phrase in quotation marks and use commas to separate the phrases. For example, `"purchase product", "MAC", "Norton SystemWorks"` searches for all three phrases, and finds all articles that include any of these phrases.
- 3 Select the area of the Web site that you want to search.
- 4 Click **Search**.

Troubleshoot Norton AntiVirus

Check here for possible solutions to issues that might arise with Norton AntiVirus.

Auto-Protect does not load when I start my computer

If the Norton AntiVirus Auto-Protect icon does not appear in the lower-right corner of the Windows taskbar, Auto-Protect is not loaded. There are three likely reasons that this is happening.

You may have started Windows in safe mode. Windows restarts in safe mode if the previous shutdown did not complete successfully. For example, you may have turned off the power without choosing Shut Down on the Windows Start menu.

To restart Windows

- 1 On the Windows taskbar, click **Start > Shut Down**.
- 2 In the Shut Down Windows dialog box, click **Restart**.
- 3 Click **OK**.

Norton AntiVirus may not be configured to start Auto-Protect automatically.

To set Auto-Protect to start automatically

- 1 In the main window, click **Options**.
If a menu appears, click **Norton AntiVirus**.
- 2 In the Options window, under System, click **Auto-Protect**.
- 3 Ensure that Start Auto-Protect when Windows starts up is checked.

Norton AntiVirus may not be configured to show the Auto-Protect icon in the tray.

To show the Auto-Protect icon in the tray

- 1 In the main window, click **Options**.
If a menu appears, click **Norton AntiVirus**.
- 2 In the Options window, under System, click **Auto-Protect**.

- 3 Ensure that Show the Auto-Protect icon in the tray is checked.

I have scanned and removed a virus, but it keeps infecting my files

There are four possible reasons a virus could be reappearing.

The virus might be in a program file with an unusual extension for which Norton AntiVirus is not configured to look.

To reset Norton AntiVirus scanning options

- 1 In the main window, click **Options**.
If a menu appears, click **Norton AntiVirus**.
- 2 In the Options window, under System, click **Manual Scan**.
- 3 Under Which file types to scan for viruses, click **Comprehensive file scanning**.
- 4 Click **Manual Scan > Bloodhound**.
- 5 Ensure that Enable Bloodhound heuristics is checked, then click **Highest level of protection**.
- 6 Click **OK**.
- 7 Scan all of the disks that you use and repair all infected files.

The source of the infection could also be a floppy disk. Scan all of the floppy disks that you use to ensure that they are free of viruses.

See "If you need to use Rescue Disks to restore your system" on page 53.

Another reason could be that the virus is remaining in memory after you remove it from the *boot record*. It then reinfects your boot record. Use your Rescue Disks to remove the virus.

If the problem is a Trojan horse or worm that was transmitted over a shared network drive, you must disconnect from the network or password protect the drive to let Norton AntiVirus delete the problem.

Norton AntiVirus cannot repair my infected files

See [“Keeping current with LiveUpdate”](#) on page 69.

The most common reason that Norton AntiVirus cannot repair your infected files is that you do not have the most current virus protection on your computer. Update your virus definitions regularly to protect your computer from the latest viruses.

If after using LiveUpdate the virus still cannot be repaired, the file may be corrupted, or contain a new virus. There are two additional options:

See [“If Norton AntiVirus places files in Quarantine”](#) on page 93.

- Quarantine the file and submit it to Symantec.
- If you don't need the file or a non-infected copy of the file exists, delete the infected file and replace it with the non-infected file.

I can't receive email messages

There are several possible solutions to this problem.

If you are using a firewall, it may block access to the Internet features of Norton AntiVirus.

Temporarily disable email protection. This might allow the problem email messages to download so that you can once again enable email protection. You are protected by Auto-Protect while email protection is disabled.

To temporarily disable incoming email protection

- 1 In the main window, click **Options**.
If a menu appears, click **Norton AntiVirus**.
- 2 In the Options window, under Internet, click **Email**.
- 3 Uncheck **Scan incoming Email**.
- 4 Click **OK**.
- 5 Download your email messages.
- 6 Reenable incoming email protection.

See [“About System options”](#) on page 62.

Your email client may have timed out. Make sure that timeout protection is enabled.

If you continue to experience problems downloading email messages, disable email protection.

To disable email protection

- 1 In the main window, click **Options**.
If a menu appears, click **Norton AntiVirus**.
- 2 In the Options window, under Internet, click **Email**.
- 3 Uncheck **Scan incoming Email**.
- 4 Uncheck **Scan outgoing Email**.
- 5 Click **OK**.

I can't send email messages

If you get the message Norton AntiVirus was unable to send your email message because the connection to your email server was disconnected, your email client may be set to automatically disconnect after sending and receiving mail.

If you are using a firewall, it may block access to the Internet features of Norton AntiVirus.

For Norton AntiVirus to scan outgoing email messages for viruses, it intercepts and scans the messages before they are sent to your email provider. To resolve this issue, turn off this option within your email client. Consult your email client manual for instructions on how to do this, or disable Norton AntiVirus outgoing email scanning.

To disable outgoing email scanning

- 1 In the main window, click **Options**.
If a menu appears, click **Norton AntiVirus**.
- 2 In the Options window, under Internet, click **Email**.
- 3 Uncheck **Scan outgoing Email**.
- 4 Click **OK**.

Troubleshoot Rescue Disks

Check here for possible solutions to issues that might arise with Rescue Disks.

My Rescue Disk does not work

See ["Create and use Rescue Disks"](#) on page 49.

Due to the number of product-specific technologies used by manufacturers to configure and initialize hard drives, the Rescue program cannot always create a bootable disk automatically. If your Rescue Boot Disk does not work properly, do one of the following:

- Be sure you have downloaded the latest Rescue Disk update from LiveUpdate.
- If you have a special startup disk for your computer, add it to your Rescue Disk set. In an emergency, start from that disk. Remove the disk and insert your Rescue Boot Disk. At the DOS prompt, type **A:RSHELL**, press Enter, then follow the on-screen instructions.
- Use the Disk Manager or similarly named program that came with your computer to make your Rescue Boot Disk bootable. Make sure to test your modified Rescue Boot Disk.

Sometimes, your Rescue Boot Disk does not work properly because you have more than one operating system installed, such as Windows 2000 and Windows 98.

To modify your Rescue Boot Disk

- 1 Start up from your hard drive.
- 2 Insert your Rescue Boot Disk into drive A.
- 3 At the DOS prompt, type **SYS A:**
- 4 Press **Enter**.
 This transfers the operating system to the Rescue Boot Disk. Be sure to retest your Rescue Disks.

I cannot start from drive A

See ["Create and use Rescue Disks"](#) on page 49.

If your computer does not check drive A first on startup, use your computer's Setup program to change settings.

Be careful when making changes using your computer's Setup program. If you have never used it before, you may want to refer to your computer manufacturer's documentation.

To change your computer's settings

- 1 Restart your computer.
A message appears telling you the key or keys to press to run SETUP, such as Press if you want to run SETUP.
- 2 Press the key or keys to launch the Setup program.
- 3 Set the Boot Sequence to boot drive A first and drive C second.
Setup programs vary from one manufacturer to the next. If you cannot find the Boot Sequence option, use the Setup program's Help system, refer to the documentation that came with your system, or contact your system's manufacturer.
- 4 Save the changes, then exit the Setup program.

You may need to use a special boot disk rather than the Rescue Boot Disk. In this case, use the boot disk or startup disk that came with your computer.

See ["My Rescue Disk does not work"](#) on page 113.

If your computer is set up with more than one operating system, such as Windows 2000 and Windows 98, you may need to modify the Rescue Boot Disk.

I get an error when testing basic Rescue Disks

See [“Create and use Rescue Disks”](#) on page 49.

If you get the message Non-system disk, replace the disk and press any key when testing your Rescue Disks, the Rescue program may not have prepared the floppy boot files correctly.

To repair the Rescue Boot Disk without having to reformat the disk and create a new Rescue Disk set

- 1 Remove the Rescue Boot Disk and restart your computer.
- 2 Insert the Rescue Boot Disk into the floppy disk drive.
- 3 On the Windows taskbar, click **Start > Run**.
- 4 In the Run dialog box, type **SYS A:**
- 5 Click **OK**.



Service and support solutions

The Service & Support Web site at <http://service.symantec.com> supports Symantec products. Customer Service helps with nontechnical issues such as orders, upgrades, replacements, and rebates. Technical Support helps with technical issues such as installing, configuring, or troubleshooting Symantec products.

Methods of technical support and customer service can vary by region. For information on support offerings in your region, check the appropriate Web site listed in the sections that follow.

If you received this product when you purchased your computer, your computer manufacturer may be responsible for providing your support.

Customer service

The Service & Support Web site at <http://service.symantec.com> tells you how to:

- Subscribe to Symantec newsletters.
- Locate resellers and consultants in your area.
- Replace defective CD-ROMs and manuals.
- Update your product registration.
- Find out about orders, returns, or a rebate status.
- Access Customer Service FAQs.
- Post a question to a Customer Service representative.
- Obtain product information, literature, or trialware.

For upgrade orders, visit the Symantec Store at:
<http://www.symantecstore.com>

Technical support

Symantec offers two technical support options for help with installing, configuring, or troubleshooting Symantec products:

- **Online Service and Support**
Connect to the Symantec Service & Support Web site at <http://service.symantec.com>, select your user type, and then select your product and version. You can access hot topics, Knowledge Base articles, tutorials, contact options, and more. You can also post a question to an online Technical Support representative.
- **PriorityCare telephone support**
This fee-based (in most areas) telephone support is available to all registered customers. Find the phone number for your product at the Service & Support Web site. You'll be led through the online options first, and then to the telephone contact options.

Support for old and discontinued versions

When Symantec announces that a product will no longer be marketed or sold, telephone support is discontinued 60 days later. Technical information may still be available through the Service & Support Web site at:
<http://service.symantec.com>

Subscription policy

If your Symantec product includes virus, firewall, or Web content protection, you may be entitled to receive updates via LiveUpdate. Subscription length varies by Symantec product.

After your initial subscription ends, you must renew it before you can update your virus, firewall, or Web content protection. Without these updates, you will be vulnerable to attacks.

When you run LiveUpdate near the end of your subscription period, you are prompted to subscribe for a nominal charge. Simply follow the instructions on the screen.

Worldwide service and support

Technical support and customer service solutions vary by country. For Symantec and International Partner locations outside of the United States, contact one of the service and support offices listed below, or connect to <http://service.symantec.com> and select your region under Global Service and Support.

Service and support offices

North America

Symantec Corporation
555 International Way
Springfield, OR 97477
U.S.A.

<http://www.symantec.com/>

Australia and New Zealand

Symantec Australia
Level 2, 1 Julius Avenue
North Ryde, NSW 2113
Sydney
Australia

http://www.symantec.com/region/reg_ap/
+61 (2) 8879-1000
Fax: +61 (2) 8879-1001

Europe, Middle East, and Africa

Symantec Authorized Service Center
Postbus 1029
3600 BA Maarssen
The Netherlands

http://www.symantec.com/region/reg_eu/
+353 (1) 811 8032

Latin America

Symantec Brasil
Market Place Tower
Av. Dr. Chucri Zaidan, 920
12º andar
São Paulo – SP
CEP: 04583-904
Brasil, SA

Portuguese:
<http://www.service.symantec.com/br>
Spanish:
<http://www.service.symantec.com/mx>
Brazil: +55 (11) 5189-6300
Mexico: +52 55 5322 3681 (Mexico DF)
01 800 711 8443 (Interior)
Argentina: +54 (11) 5382-3802

June 3, 2003

Glossary

access privileges	The types of operations that a user can perform on a system resource. For example, a user can have the ability to access a certain directory and open, modify, or delete its contents.
ActiveSync	The synchronization software for Microsoft Windows-based Pocket PCs.
ActiveX	A method of embedding interactive programs into Web pages. The programs, which are called controls, run when you view the page.
alert	A message that appears to signal that an error has occurred or that there is a task that requires immediate attention, such as a system crash or a Virus Alert.
alias	A shortcut icon that points to an original object such as a file, folder, or disk.
AppleTalk	A protocol that is used by some network devices such as printers and servers to communicate.
attack signature	A data pattern that is characteristic of an Internet attack. Intrusion Detection uses attack signatures to distinguish attacks from legitimate traffic.
beam	To transfer certain programs and data between two handheld devices using built-in infrared technology.

boot record	A sector at the start of a disk that describes the disk (sector size, cluster size, and so on). On startup disks, the boot record also has a program that loads the operating system.
bootable disk	A disk that can be used to start a computer.
cache	A location on your disk in which data is stored for reuse. A Web browser cache stores Web pages and files (such as graphics) as you view them.
cache file	A file that is used to improve the performance of Windows.
compressed file	A file whose content has been made smaller so that the resulting data occupies less physical space on the disk.
connection-based protocol	A protocol that requires a connection before information packets are transmitted.
connectionless protocol	A protocol that sends a transmission to a destination address on a network without establishing a connection.
cookie	A file that some Web servers put on your disk when you view pages from those servers. Cookies store preferences, create online shopping carts, and identify repeat visitors.
denial-of-service attack	A user or program that takes up all of the system resources by launching a multitude of requests, leaving no resources, and thereby denying service to other users.
DHCP (Dynamic Host Configuration Protocol)	A TCP/IP protocol that assigns a temporary IP address to each device on a network. DSL and cable routers use DHCP to allow multiple computers to share a single Internet connection.
dial-up	A connection in which a computer calls a server and operates as a local workstation on the network.

DNS (Domain Name System)	The naming system used on the Internet. DNS translates domain names (such as www.symantec.com) into IP addresses that computers understand (such as 206.204.212.71).
DNS server (Domain Name System server)	A computer that maps domain names to IP addresses. When you visit www.symantec.com , your computer contacts a DNS server that translates the domain name into an IP address (206.204.212.71).
domain	The common Internet address for a single company or organization (such as symantec.com). See also host name.
DOS window	A method of accessing the MS-DOS operating system to execute DOS programs through the Windows graphical environment.
download	To transfer a copy of a file or program from the Internet, a server, or computer system to another server or computer.
driver	Software instructions for interpreting commands for transfer to and from peripheral devices and a computer.
encryption	Encoding data in such a way that only a person with the correct password or cryptographic key can read it. This prevents unauthorized users from viewing or tampering with the data.
Ethernet	A common method of networking computers in a LAN (local area network). Ethernet cables, which look like oversized phone cables, carry data at 10M bps or 100M bps.
executable file	A file containing program code that can be run. Generally includes any file that is a program, extension, or system files whose names end with .bat, .exe, or .com.

extension	The three-letter ending on a file name that associates the file with an activity or program. Examples include .txt (text) and .exe (executable program).
FAT (file allocation table)	A system table (used primarily by DOS and Windows 9x/Me) that organizes the exact location of the files on the hard drive.
file type	A code that associates the file with a program or activity, often appearing as the file name extension, such as .txt or .jpeg.
Finder	The program that manages your Macintosh disk and file activity and display.
firewall rule	Parameters that define how a firewall reacts to specific data or network communications. A firewall rule usually contains a data pattern and an action to take if the pattern is found.
fragmented	When the data that makes up a file is stored in noncontiguous clusters across a disk. A fragmented file takes longer to read from the disk than an unfragmented file.
fragmented IP packet	An IP packet that has been split into parts. Packets are fragmented if they exceed a network's maximum packet size, but malicious users also fragment them to hide Internet attacks.
FTP (File Transfer Protocol)	An application protocol used for transferring files between computers over TCP/IP networks such as the Internet.
hidden attribute	A file attribute that makes files harder to access and more difficult to delete than other files. It also prevents them from appearing in a DOS or Windows directory list.
host name	The name by which most users refer to a Web site. For example, www.symantec.com is the host name for the Symantec Web site. Host names are translated to IP addresses by the DNS.

HotSync	The synchronization software for Palm OS handheld devices.
HTML (Hypertext Markup Language)	The language used to create Web pages.
ICMP (Internet Control Message Protocol)	An extension to the basic Internet Protocol (IP) that provides feedback about network problems.
IGMP (Internet Group Management Protocol)	An extension to the basic Internet Protocol (IP) that is used to broadcast multimedia over the Internet.
IMAP4 (Internet Message Access Protocol version 4)	One of the two most popular protocols for receiving email. IMAP makes messages available to read and manage without downloading them to your computer.
infrared (IR) port	A communication port on a handheld device for interfacing with an infrared-capable device. Infrared ports do not use cables.
IP (Internet Protocol)	The protocol that underlies most Internet traffic. IP determines how data flows from one computer to another. Computers on the Internet have IP addresses that uniquely identify them.
IP address (Internet Protocol address)	A numeric identifier that uniquely identifies a computer on the Internet. IP addresses are usually shown as four groups of numbers separated by periods. For example, 206.204.52.71.
ISP (Internet service provider)	A company that supplies Internet access to individuals and companies. Most ISPs offer additional Internet connectivity services, such as Web site hosting.
Java	A programming language used to create small programs called applets. Java applets can be used to create interactive content on Web pages.

JavaScript	A scripting language used to enhance Web pages. Most sites use JavaScript to add simple interactivity to pages, but some use it to open pop-up ads and reset visitors' hompages.
macro	A simple software program that can be started by a specific keystroke or a series of keystrokes. Macros can be used to automate repetitive tasks.
NAT (network address translation)	A method of mapping private IP addresses to a single public IP address. NAT allows multiple computers to share a single public IP address. Most DSL and cable routers support NAT.
network address	The portion of an IP address that is shared by all computers on a network or subnet. For example, 10.0.1.1 and 10.0.1.8 are part of the network address 10.0.1.0.
NTFS (NTFS file system)	A system table (used primarily by Windows 2000/XP) that organizes the exact location of all the files on the hard drive.
packet	The basic unit of data on the Internet. Along with the data, each packet includes a header that describes the packet's destination and how the data should be processed.
partition	A portion of a disk that is prepared and set aside by a special disk utility to function as a separate disk.
POP3 (Post Office Protocol version 3)	One of the two most popular protocols for receiving email. POP3 requires that you download messages to read them.
port	A connection between two computers. TCP/IP and UDP use ports to indicate the type of server program that should handle a connection. Each port is identified by a number.

port number	A number used to identify a particular Internet service. Internet packets include the port number to help recipient computers decide which program should handle the data.
PPP (Point-to-Point Protocol)	A protocol for communication between two computers using a dial-up connection. PPP provides error-checking features.
protocol	A set of rules governing the communication and transfer of data between computers. Examples of protocols include HTTP and FTP.
proxy	A computer or program that redirects incoming and outgoing traffic between computers or networks. Proxies are often used to protect computers and networks from outside threats.
registry	A category of data stored in the Windows registry that describes user preferences, hardware settings, and other configuration information. Registry data is accessed using registry keys.
removable media	Disks that can be removed, as opposed to those that cannot. Some examples of removable media are floppy disks, CDs, DVDs, and Zip disks.
router	A device that forwards information between computers and networks. Routers are used to manage the paths that data takes over a network. Many cable and DSL modems include routers.
script	A program, written in a scripting language such as VBScript or JavaScript, that consists of a set of instructions that can run without user interaction.
service	General term for the process of offering information access to other computers. Common services include Web service and FTP service. Computers offering services are called servers.

SSL (Secure Sockets Layer)	A protocol for secure online communication. Messages sent using SSL are encrypted to prevent unauthorized viewing. SSL is often used to protect financial information.
subnet	A local area network that is part of a larger intranet or the Internet.
subnet mask	A code, in the form of an IP address, that computers use to determine which part of an IP address identifies the subnet and which part identifies an individual computer on that subnet.
synchronize	The process by which a handheld device and computer compare files to ensure that they contain the same data.
TCP/IP (Transmission Control Protocol/ Internet Protocol)	Standard protocols used for most Internet communication. TCP establishes connections between computers and verifies that data is properly received. IP determines how the data is routed.
threat	A program with the potential to cause damage to a computer by destruction, disclosure, modification of data, or denial of service.
Trojan horse	A program containing malicious code that is disguised as or hiding in something benign, such as a game or utility.
UDP (User Datagram Protocol)	A protocol commonly used for streaming media. Unlike TCP, UDP does not establish a connection before sending data and it does not verify that the data is properly received.
virus definition	Virus information that an antivirus program uses to identify and alert you to the presence of a specific virus.

wildcard characters

Special characters (like *, \$, and ?) that act as placeholders for one or more characters. Wildcards let you match several items with a single specification.

worm

A program that replicates without infecting other programs. Some worms spread by copying themselves from disk to disk, while others replicate only in memory to slow a computer down.



Index

A

- activation 20, 42
 - and registration of software 35
 - key 31
 - window 31
- Activity Log
 - checking 47
 - viewing 47
- adding files to Quarantine 94
- Adobe Acrobat Reader
 - installing 56
 - using to view PDF 56
- alerts
 - Inoculation 93
 - Worm Blocking 92
- at-risk files
 - about 89
 - excluding 89
- Automatic LiveUpdate 64, 74
- Auto-Protect
 - description 43
 - disabling 43, 50
 - enabling 43, 77
 - failure to load on startup 109
 - functions 21
 - options 63

B

- backing up files before repair 65
- Bloodhound technology
 - description 22

Bloodhound technology (*continued*)

- options 63
- booting
 - Auto-Protect failure to load 109
 - changing floppy disk drive settings 114
 - floppy disk drive fails 114
 - Rescue Disks fail 113

C

- CD-ROM drive
 - about 13
 - starting from 13
- changing
 - floppy disk drive settings 115
 - scan schedules 85
- checking
 - for recoverable files 99
 - system status 45
 - version number 39
- computer
 - emergency procedures 11
 - requirements 25
- connecting to the Internet
 - automatically 74
- creating
 - Emergency Disks 14
 - Rescue Disks 49
- custom scans
 - changing schedule 85
 - creating 81

custom scans (*continued*)

- deleting 83
- deleting schedule 86
- running 83
- scheduling 83, 84
- using 81

D

data

- eliminating permanently 101, 104
- recovering erased 97

default options 66

definitions of technical terms 55

deleting

- custom scans 83
- infected files 90
- scan schedules 86

description of product features 19

disabling

- Automatic LiveUpdate 75
- Auto-Protect 43

disks

- manually scanning 79
- protecting 77
- scanning for viruses 79

displaying the Norton AntiVirus

toolbar 41

E

electronic newsletter 59

eliminating data permanently 101

email

- options 64
- protection 64

emergency

- preparations 17
- recovery procedures 11

Emergency Disks

- creating 14
- using 15

enabling

- Automatic LiveUpdate 72
- Auto-Protect 43
- Office Plug-in 65

erased files

- about 97
- recovering 99

excluding at-risk files 87, 89

Express mode for LiveUpdate 72

F

FAQs 109

features

- Information Wizard 34
- Norton AntiVirus 19, 21

file extensions

- about 95
- unusual 110

files

- adding to Quarantine 94
- and Norton Protection 97
- check if recoverable 99
- recovering 97
- reinfected after virus removal 110
- security considerations 101

firewall

- and LiveUpdate 73
- and network 73

floppy drives

- about 114
- unable to boot from 114

folders

- creating for Rescue Disks 50
- scanning for viruses 79

full system scans 79

G

glossary 55

H

Help

online 55

window and dialog box 55

hexadecimal values in Wipe Info 102

I

ignoring files 91

infected files

cannot repair 111

reinfected 110

Information Wizard

features 35

using 35

when it appears 34

Inoculation

alerts 93

options 65

responding to alerts 93

installing Norton AntiVirus 28

instant messenger

options 64

scanning transferred files 77

virus protection 22

Interactive mode for LiveUpdate 72

Internet

Knowledge Base articles 107

options 63

Symantec service and support

Web site 107

Symantec Web sites 57

Intrusion Detection

service 70

updates 70

italicized terms 55

L

LiveUpdate

Interactive and Express modes 72

options 64

Log Viewer

contents 47

monitoring activities in 47

M

Miscellaneous options 64, 65

N

networks

internal LiveUpdate server 73

using LiveUpdate 73

new features in Norton AntiVirus 21

newsletters 59

Norton AntiVirus

Auto-Protect 21

Bloodhound technology 22

customizing 62

starting from the main

window 40

starting from the Windows

Explorer toolbar 40

starting from the Windows system

tray 40

virus protection 21

virus protection updates 21

Norton Protection 97

O

Office Plug-in

enabling 65

status 46

online

Help 55

Virus Encyclopedia 96

operating systems

multiple 113

required for installation 25

- options 61
 - Auto-Protect
 - Advanced 63
 - Bloodhound 63
 - Exclusions 63
 - categories 62
 - changing 65
 - changing settings for 62
 - customizing 62
 - email
 - Advanced 64
 - scanning 64
 - Inoculation 65
 - instant messenger 64
 - Internet 63
 - LiveUpdate 64
 - Manual Scan
 - Bloodhound 63
 - Exclusions 63
 - Miscellaneous 64, 65
 - Other 64
 - password protection in Norton
 - AntiVirus 22
 - resetting defaults 66
 - Threat Categories 65
 - Wipe Info 103
 - Worm Blocking 64
- Other options 64

P

- password protection option 65
- problems
 - troubleshooting Norton
 - AntiVirus 109
 - troubleshooting Rescue
 - Disks 113
- product key 20
- program
 - patches 69
 - updates 69

- protection
 - downloading from Symantec Web
 - site 71
 - maintaining 16
 - maximum 77
 - preparing for emergencies 17
 - system scans 79
 - updates 70
 - updating automatically 74

Q

- Quarantine
 - actions in 94
 - adding files to 94
 - files in 93
 - infected files in 90
 - options 93
 - restoring items 94

R

- Readme file 56
- Recycle Bin
 - and Norton Protection 97
 - recovering files 99
- registering your software 35
- removing
 - Norton AntiVirus from your
 - computer 38
 - other antivirus programs 28
 - previous copies of Norton
 - AntiVirus 28
- Repair Wizard 88
- repairing
 - infected files
 - in Windows 2000/XP 91
 - in Windows 98/98SE/Me 90
 - viruses 21
- required computer configuration 25
- Rescue Disks
 - creating 49
 - creating folder on hard disk 50

Rescue Disks (*continued*)

- disabling Auto-Protect 50
- failure to start from 113
- not current 54
- supported platforms 49
- testing 51
- troubleshooting 113
- updating 52
- using 53

restarting

- after installing 34
- Windows in safe mode 109

restoring

- items in Quarantine 94
- system with Rescue Disks 53

S

safe mode 109

scan summary 88

scanning

- automatically 83
- before installation 29
- email messages 64
- entire computer 79
- files at startup 65
- individual elements 80
- problems found during 81

scans

- creating custom 81
- deleting custom 83
- file 80
- floppy disk 80
- folder 80
- full system 79
- hard drive 80
- removable drive 80
- running custom 83
- using custom 81

scheduling

- custom scans 84
- multiple schedules for a scan 84
- virus scans 83

Secure Sockets Layer (SSL)

- connections 27

security risks

- about 87
- finding 87

Service and Support 117

Setup program

- about 114
- changing boot drive sequence 114

starting

- from the CD-ROM drive 13
- Norton AntiVirus 40

startup

- alert about virus protection 65
- Auto-Protect failure to load 109
- changing floppy disk drive settings 114
- floppy disk drive fails 114
- Rescue Disks fail 113
- scanning files at 65

submitting files to Symantec 94

subscription to product updates 76

summary of product features 19

Symantec Pre-Install Scanner 29

Symantec Security Response

- newsletter 59
- Web page 41, 58

Symantec service and support Web site 107

Symantec Web sites 57, 71

- connecting to 41
- look up viruses 96

system

- requirements 25
- status, checking 45

T

Technical Support 57, 117

threats

- avoiding 16
- expanded detection 21

- timeout protection 78
- toolbar
 - displaying Norton AntiVirus from 41
 - viewing the Virus Encyclopedia from 58
- Trojan horses
 - found during a scan 88
 - transmitted over a network 110
- troubleshooting 107, 109
 - recovering erased files 97
 - Rescue Disk problems 113

U

- UnErase Wizard
 - features 23, 98
 - recovering files 99
- uninstalling
 - Norton AntiVirus 38
 - other antivirus programs 28
 - previous copies of Norton AntiVirus 28
- unknown viruses 22
- updating
 - from Symantec Web site 71
 - Rescue Disks 52
 - virus protection 71
- User's Guide PDFs
 - on CD 56
 - opening 57

V

- version number
 - about 39
 - checking 39
- virus alert options 90
- Virus Encyclopedia 41, 58
- virus protection
 - alerts 65
 - system scans 79
 - updates 21

- virus repair
 - in Windows 2000/XP 91
 - in Windows 98/98SE/Me 90
- viruses
 - automatic protection 21
 - avoiding 16
 - descriptions 21
 - found by Auto-Protect 90
 - found during a scan 88
 - looking up on the Symantec Web site 96
 - submitting to Symantec 94
 - unknown 22
 - viewing descriptions 96

W

- Web
 - filtering service 70
 - sites, Symantec 57, 71, 107
- Windows
 - operating systems 25
 - safe mode 109
 - system tray icon 44
- Windows 2000
 - virus repair 91
 - Wipe Info procedure 104
- Windows Explorer toolbar
 - displaying Norton AntiVirus 40
 - viewing the Virus Encyclopedia from 58
- Windows XP
 - System Restore after Wipe Info 101
 - Wipe Info procedure 104
- Wipe Info
 - and Windows Me/XP System Restore 101
 - characters used to wipe 102
 - defined 101
 - features 23, 101
 - Government Wipe 102
 - on Windows 2000/XP 104

- Wipe Info (*continued*)
 - options 103
 - procedures 101, 104
 - wizard 101
- wizards
 - Information 35
 - Repair 88
 - UnErase 98
 - Wipe Info 101
- Worm Blocking
 - monitoring by 77
 - Norton AntiVirus 22
 - options 64
 - threats found by 92
- worms
 - found by Worm Blocking 92
 - found during a scan 88